

IBM Content Manager Enterprise Edition
IBM Content Manager for z/OS
Version 8.4.3

System Administration Guide



IBM Content Manager Enterprise Edition
IBM Content Manager for z/OS
Version 8.4.3

System Administration Guide



Note

Before using this information and the product it supports, read the information in “Notices” on page 707.

This edition applies to version 8, release 4, modification 3 of IBM Content Manager Enterprise Edition (product number 5724-B19) and version 8, release 4, modification 3 of IBM Content Manager for z/OS (product number 5697-H60) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 1993, 2011.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

ibm.com and related resources	ix
How to send your comments	ix
Contacting IBM	x

Accessibility features of IBM Content Manager 1

Keyboard input and navigation	1
Keyboard shortcut keys.	1
Features for accessible display	3
Compatibility with assistive technologies	3
Accessible documentation	3
eClient accessibility	4

Defining and configuring a library server 5

Library server	5
Viewing or modifying the library server configuration	6
Single sign-on options	11
Creating a language definition	12
Language definition	12
Language codes	13
Additional language definitions	14
Changing the library server and system administrator password to the resource manager	16
Login user exit scenarios	17
Verify whether a user exit routine is being invoked	24
Checking which user ID is being used as the shared connection ID	25
Changing the ACL optimization mode	25
Access control list optimization modes for the entries in the ICMSTCompiledACL table	27
Running performance testing for the ACL optimization modes	29

Connecting content servers to IBM Information Integrator for Content 31

Defining servers	32
Defining server types	33
Connectors	33
Defining connection and configuration strings.	33
Defining an IBM Content Manager Version 8 server	34
Defining an ImagePlus for OS/390 server	35
Tracing in IBM Content Manager ImagePlus for OS/390.	35
Defining the Content Manager OnDemand server	36
Working with the Content Manager OnDemand connector TCP/IP tuning and sockets	37
Defining an IBM Content Manager for AS/400 server	38
Connecting to multiple Content Manager for AS/400 servers	38
Viewing or modifying an existing content server definition	38

Copying a content server definition	39
---	----

Defining and configuring resource managers in IBM Content Manager 41

Resource manager	41
Resource manager background services	44
Resource managers on z/OS.	44
Testing the SSL connection	47
Defining a resource manager	48
Defining a resource manager on z/OS	50
LAN cache	51
Adding an access type.	53
Viewing or modifying the staging area properties	54
Staging area	55
Creating resource manager configurations	56
Resource manager configuration	60
Adding a server definition	61
Server definition.	62
Content encryption with Tivoli Storage Manager	64
Configuring a lockout for resource manager logon failures	65
Releasing the resource manager lockout	66

Connecting the system administration client to the databases 67

Connecting to a remote database	67
Locating the remote database connection information	68
Using the server configuration utility.	70
Manually connecting to a remote DB2 database	72
Database connection parameter file	75

Developing federated searches with IBM Information Integrator for Content 79

Mapping native and federated data	79
Creating a federated entity with the wizard	79
Creating a federated entity manually	83
Search template	91
Defining a search template with the wizard	92
Creating a search template manually	95
Deleting definitions	100
Assigning applications for view and launch of native data	100
MIME types.	100
Adding a MIME type editor	101
Adding a MIME type association.	101

Getting started with content management administration 103

Getting started with IBM Content Manager administration	103
Launching <i>First Steps</i> for IBM Content Manager	104
Getting started with IBM Information Integrator for Content administration	105

System administration client	106
Display name	107
Product names	107
Supported document formats	108

Logging on to the system

administration client 117

Starting the system administration client on UNIX	117
Starting the system administration client on Windows	117
Combined administration	118
Changing your password	119

Modeling your data in IBM Content

Manager 123

Planning your data model	125
Step 1: Identify your data	125
Step 2: Separate your data into operational and non-operational	127
Step 3: Sort your data into like types	129
Step 4: Identify your users and what data they need to access	130
Step 5: Within each data type, identify the elements that might be searched for	132
Step 6: Identify hierarchies and elements that might have multiple values.	133
Step 7: Diagram data relationships	134
Step 8: Decide whether you require a custom data model	135
Step 9: Map your diagrammed data to an IBM Content Manager data model	136
Creating an attribute	146
Attributes	148
Defining a display name	149
Creating an attribute group.	151
ICM\$NAME attribute	152
Creating an item type	153
Item type.	156
Selecting an access control list for the item type	162
Adding attributes and attribute groups to the item type.	163
Filtering objects from display in IBM Content Manager	169
Specifying default storage for the item type	170
Logging item type events	170
Defining document management relations.	171
Specifying user exit routines	172
Forming relationships between items	173
Defining a link type	174
Creating a reference attribute	176
Defining a foreign key	178
Enabling auto-linking	187
Defining data model options	190
Defining a semantic type	190
Defining a MIME type	192
Creating a media object (XDO) class.	195
Creating a database index	198
Creating an item type subset	200
Defining text search options	202
Exporting data as XML	218

Exporting item types to a WSDL file	220
Importing data	221
Importing data from XML	222
Resolving import conflicts	224
Import selection confirmation	225
Mapping and importing XML schemas into IBM Content Manager	225
Creating an XML schema file	226
Validating a storage schema	228
Importing a storage schema	231
Creating a query	231
Saving your mapping	231
XML schema mapping tool interface.	232
Using the Content Manager for z/OS high-volume batch load utility	238
Using the Content Manager for z/OS high-volume batch update utility	240
Deferring DDL execution	241
Enabling the deferred DDL execution feature.	242
Scripts to create an item type	243
Changing library server configurations when DDL deferred execution feature is enabled	245
Allowing IBM Content Manager administrators without DB2 dbadm privilege to create the definition of data model objects	245
Enabling the deferred DDL execution feature for Oracle.	246

Managing document routing with IBM

Content Manager. 253

Planning a document routing process	256
Planning process flow	256
Planning work assignments	258
Planning user and system interaction throughout process	264
Creating a document routing process	265
Prerequisite tasks	265
Defining an action list	269
Defining work nodes outside of the graphical process builder.	275
Modeling the process graphically.	294
Creating a worklist	312
Establishing automatic workflow	317

Managing object storage in IBM

Content Manager. 319

Object storage	320
Object storage load balancing	321
Creating a storage class	323
Storage class.	323
Creating a device manager	325
Device manager	326
Creating and enabling the ICMZFS device manager	326
Creating and enabling the TSMPOOLED device manager	327
Device managers by operating system or product	328
Creating a storage system	329
Storage system	329

Creating a NAS volume	331
Creating a local storage volume	333
Creating a DB2 Content Manager VideoCharger volume	338
Creating a media archive volume.	341
Creating a Tivoli Storage Manager volume	342
Deleting a storage system	347
Replacing or repartitioning a hard disk.	347
Creating a storage group	350
Storage group	350
Creating a migration policy.	352
Migration policy	352
Creating a migration policy entry.	354
Changing the date of migration	355
Migrating and purging the DB2 Content Manager VideoCharger Server media objects at regular intervals	355
Creating a collection	356
Selecting a target resource manager and collection.	357
Defining OAM collections	357
Defining Tivoli Storage Manager collections on z/OS	358
Collection	360
Setting up replication.	362
Replication	364
Turning on replication for objects that have already been stored	364
Defining replication rules in administrative domains	366
Library server monitor fail-over service.	366
Cataloging objects from your local system.	367
Backing up and restoring your data	368
Pausing IBM Content Manager for backups	368
Resuming IBM Content Manager after backups	369

Managing servers in IBM Content Manager 371

Starting and stopping a resource manager.	371
Starting and stopping a resource manager on AIX	371
Starting and stopping a resource manager on Linux	372
Starting and stopping a resource manager on Solaris.	373
Starting and stopping a resource manager on Windows.	374
Starting and stopping the HTTP server that runs the z/OS resource manager	375
Resource manager startup behavior	375
Changing ownership of the resource manager	376
Starting and stopping resource manager services	376
Finding data discrepancies with the validation utility	377
Resource manager validation utilities	378
Validation utility discrepancy reports	378
Saving validation utility discrepancy reports as XML files.	380
Using the APIs for validation utility scheduling	381
Repairing data discrepancies with the validation utility recovery tools	383

IBM Content Manager data validation utility for z/OS	393
Managing databases	394
Optimizing server databases	395
Analyzing a DB2 database for optimization	395
z/OS resource manager exit programs	396
Logging and tracing for IBM Content Manager	396
Specifying log settings for IBM Content Manager components.	397
Enabling tracing in IBM Content Manager.	406
Enabling tracing in Content Manager for z/OS	410
Enabling the DSNTRACE resource manager DB2 trace facility	414
Enabling the HTTP Server trace facility.	414
Event logging	414

Managing user access 427

Authenticating users	428
Managing user IDs and passwords	429
Managing users with LDAP	435
Creating users	457
Creating user groups	464
Authorizing users	467
User authorization and privileges	467
Authorizing user administrators to log on to the system administration client	469
Managing access to data.	470
Defining privileges, privilege groups, and privilege sets	476
Administering users	516
Enabling administrative domains.	516
Creating administrative domains	517
Assigning components to domains	519
Moving components from one domain to another	521

Managing advanced workflow with IBM Information Integrator for Content 525

Creating a workflow process	528
Prerequisite tasks	528
Defining an action list	532
Modeling the workflow graphically	537
Defining a worklist	559

Troubleshooting system administration 565

Troubleshooting IBM Content Manager problems with the IBM Support Assistant	566
Information collected by the Content Manager EE Enterprise Edition plug-in data collection tool.	568
Log file locations	570
Tracing errors	571
Finding IBMCMROOT	571
Troubleshooting the information center.	571
Information center does not display	572
Information center topics display in English	572
Information center readme file not found	573
Information center welcome page not found	573
Information center page not found	574

Main eClient help topic not found in information center	574	The cmbemconfig.properties file is missing some configuration data	599
Information center does not start on a system with only eClient installed	575	The cmbemconfig.properties file cannot be found or is not accessible	600
Commands to start and stop the information center not found	575	Troubleshooting the library server	600
Java error when starting the information center	576	Connection to an Oracle library server database fails	601
Information center conflict with other Windows applications	576	Query performance can be slow with a query on the SEMANTICTYPE condition	602
Troubleshooting the system administration client	577	DGL3608A error when trying to import documents into IBM Content Manager	604
Unable to view newly modified information, even after clicking Refresh	577	Cannot export an item type to a WSDL file	604
Cannot retrieve objects when using characters outside the 7-bit ASCII range	578	System failed to retrieve large objects	605
System administration client help does not work	579	ICMRM transaction management failure	606
System administration client field-level help does not always display automatically	579	Code page error during item creation	607
Troubleshooting administration client messages	579	Too many cursors returned during item retrieval	607
System administration client does not start on UNIX	582	Error DGL5390A for minimum string length violation	608
System administration client does not start on Windows	582	Error LS RC 7015 SQL RC=-911 linked to concurrency control in the IBM Content Manager database	608
System administration client logon fails	584	Failure to import XML using DKDDO.from XML().	610
System administration client logon fails after installing fix pack	589	Failure to enable database for text with DB2 Net Search Extender	610
System administrator cannot log on to z/OS	589	Failure to define an item type that has text searchable attributes	611
Invalid parameter error when creating or viewing an item type.	589	Failure to change a text index	611
OnDemand for AS/400 connection test fails	590	Determining the status of an index update that appears to have hung	612
Content Manager server inventory viewer is empty	590	Unable to index plain text documents when using the CTXSYS.INSO_FILTER or CTXSYS.AUTO_FILTER preferences for a library server using Oracle	612
Displaying non-English display names for objects in the system administration client.	591	Specifying code pages for phrased text search of Thai language content	613
Locating the IBM Content Manager database schema name using DB2 commands.	592	Unexpected text search results for Thai phrases	613
Federated entities, search templates not displayed in administration client, APIs	593	SQL0302N error when creating or updating a document	614
Server connection test fails, system returns DGL0394A	593	Table space is in check pending state after adding or editing a foreign key on z/OS only	617
Attribute sizing and string length considerations for non-English environments	593	Error loading libraries in a 64-bit environment	618
Selecting and deleting work nodes can cause slow performance	594	DGL0394A error when trying to log on to the library server with the system administration client	619
Auto-linking race condition creates duplicate folders.	595	Error LS RC 7017 SQL RC -670 row length exceeded limit	619
XML import using the process interactively option	595	Insufficient space when creating a large number of item types and item type subsets	620
JAR file clash between WebSphere Application Server and XML services	596	Changing the host name the resource manager uses to communicate with the library server	620
IBM Content Manager components stop on Linux	596	SQL error code -181: Asynchronous recovery process cannot delete the entries in ICMSTItemsToDelete table	621
Using IPv6 addresses in the system administration client	597	Transaction log file for the database is full.	621
Troubleshooting the event monitor and event handler	597	DGL0394A error when connecting to an IBM Content Manager server using the system administration client	622
An event monitor instance has already been started.	597	Troubleshooting batch load utility problems for Content Manager for z/OS	623
Encountered a database error	598	Troubleshooting the XML schema mapping tool	625
Initial context cannot be created	598		
LDAP authentication for JMS fails	599		

Troubleshooting XML schema mapping tool errors	625	Cannot retrieve documents larger than 2 MB through IBM Information Integrator for Content V8 to DB2 Content Manager V7.1 server	652
Unable to import item types with the entityView property specified in the annotation dialog box using the XML schema mapping tool	626	Configuring IBM Information Integrator for Content API logging	652
Locating an object that did not get indexed	627	Troubleshooting user authentication and access control	659
Troubleshooting the resource manager	628	Cannot define access control lists	659
Retrieving large objects from the resource manager	629	Client logon attempts causing lockouts	660
DB2 SORT errors in resource manager	629	System accounts and passwords	661
System failed to create new Tivoli Storage Manager volume	630	Error occurred while updating user	664
No suitable driver in the log file when starting the resource manager for IBM Content Manager with DB2 Universal Database	631	Error: supplied credentials invalid	664
Verifying database creation and deployment	632	Error SQL0964C when trying to enable public access	665
Troubleshooting resource manager database creation errors using the icmcrmdb.log	632	Troubleshooting LDAP integration	666
Verifying resource manager deployment	633	Finding the log files that help with LDAP troubleshooting.	666
Verifying database connections	634	Troubleshooting authentication problems with the LDAP user preauthentication tool	667
Verifying communication with the Web server	634	Running the LDAP user import utility with the correct user privileges	668
Secure Sockets Layer	635	LDAP user import scheduler save function fails	669
Resource manager is not online or available	635	Problems with the LDAP import utility schedule on non-English Windows operating systems	669
Error storing objects in Object Access Method (OAM)	637	Scheduled LDAP import does not launch on Windows.	670
Changing the resource manager port number on UNIX and Windows	637	Using log files for problem diagnosis if LDAP user authentication fails	670
Changing the resource manager port number on z/OS	638	Resource manager LDAP authentication is failing	672
Manually synchronizing the encryption key	639	Users cannot connect after you import users from LDAP	673
DB2 return code -818 during SMS interface utility processing	640	Authentication of users fails when using the common name user attribute with Active Directory	674
Deadlock error SQL0911 RC=2 when importing documents or replicating to a target resource manager	641	Incorrect password entries cause account lockouts earlier than expected	675
Error message ICM9712 failed to store documents	641	Troubleshooting document routing processes	676
Enabling the advertisement of byte serving capability for document retrieval to the clients	642	Cannot start MQ Workflow server with cmbwfstart command	676
Troubleshooting resource manager asynchronous jobs.	643	Failed to synchronize users with EIPUser2WE.bat	677
Troubleshooting database connection failures on the resource manager.	645	Failure to create workflow or retrieve workflow template	678
Troubleshooting replication.	647	Icon is reset each time the icon is dropped on the drawing surface in the workflow builder	679
Items that are checked out are not replicated	648	Workflow builder does not have work node variables listed in the Decision Point window	679
Replication return code 7400	648	Incorrect routing of first document in a workflow.	679
ChangeSMS fails on a secondary resource manager	648	Document routing performance problems during updates.	680
Cannot change or manage replication rules in the public domain.	649	Locale-specific considerations	681
Content Manager Version 8.1 client application receives library server return code 7652	650	Considerations for Lithuanian locale.	681
Cannot replicate existing items migrated from Content Manager Version 8.1	650	Considerations for Thai locale	682
Changing replication rules is not affecting existing items	651	Considerations for Turkish locale.	682
Troubleshooting IBM Information Integrator for Content	651		
Cannot add users to IBM Information Integrator for Content	651		
		Setting up your system to integrate with FileNet Business Process Manager	683

FileNet Business Process Manager integration . . .	683
Example system configuration with FileNet Business Process Manager	686
Configuring the library server for an Oracle system	687
Setting up a JMS queue in WebSphere MQ . . .	688
Setting up a JMS queue in WebSphere MQ with LDAP	690
LDAP server configuration for storing Java objects.	692
Setting up the FileNet Business Process Manager connection	693
Configuring the FileNet Business Process Manager connection in the system administration client	694
Logging on to FileNet Business Process Manager	695
Modifying the event monitor and event handler settings	696

Starting and stopping the event monitor	698
Starting and stopping the event handler	700
Subscribing to events.	701
Event subscriptions	701
Enabling IBM Content Manager item types to start a FileNet Business Process Manager process with process integration	702
Defining an event subscription for general integration	704
Updating or deleting an event subscription . .	704

Notices	707
Trademarks	709

Glossary	711
---------------------------	------------

Index	731
------------------------	------------

ibm.com and related resources

Product support and documentation are available from [ibm.com](http://www.ibm.com)[®].

Support and assistance

Product support is available on the web. Click Support from the product website at:

IBM[®] Content Manager Enterprise Edition

<http://www.ibm.com/software/data/cm/cmgr/mp/edition-enterprise.html>

IBM Content Manager for z/OS[®]

<http://www.ibm.com/software/data/cm/cmgr/390/>

Information center

You can view the product documentation in an Eclipse-based information center that you can install when you install the product. By default, the information center runs in a web server mode that other web browsers can access. You can also run it locally on your workstation. See the information center at <http://publib.boulder.ibm.com/infocenter/cmgmt/v8r4m0/index.jsp>.

PDF publications

You can view the PDF files online using the Adobe Acrobat Reader for your operating system. If you do not have the Acrobat Reader installed, you can download it from the Adobe Web site at <http://www.adobe.com>.

See the following PDF publications Web sites:

Product	Web site
IBM Content Manager Enterprise Edition	http://www.ibm.com/support/docview.wss?rs=86&uid=swg27020935
IBM Content Manager for z/OS	http://www.ibm.com/support/docview.wss?rs=119&uid=swg27020936

“How to send your comments”

“Contacting IBM” on page x

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

Send your comments by using the online reader comment form at https://www14.software.ibm.com/webapp/iwm/web/signup.do?lang=en_US&source=swg-rcf.

Consumability survey

You are invited to tell IBM how to improve the consumability of software products. If you want to help IBM make IBM Content Manager easier to use, take the Consumability Survey at <http://www.ibm.com/software/data/info/consumability-survey/>.

Contacting IBM

To contact IBM customer service in the United States or Canada, call 1-800-IBM-SERV (1-800-426-7378).

To learn about available service options, call one of the following numbers:

- In the United States: 1-888-426-4343
- In Canada: 1-800-465-9600

For more information about how to contact IBM, see the Contact IBM Web site at <http://www.ibm.com/contact/us/>.

Accessibility features of IBM Content Manager

IBM Content Manager and DB2® Content Manager VideoCharger include a number of features that make it more accessible for people with disabilities.

You can find accessibility features for other products, such as your operating system or browser, within the product information for those products.

Attention: The accessibility features are fully supported on Windows operating systems only.

The linked sections document the accessibility features.

“eClient accessibility” on page 4

Related concepts

“Compatibility with assistive technologies” on page 3

“Accessible documentation” on page 3

Related reference

“Keyboard shortcut keys”

“Keyboard input and navigation”

“Features for accessible display” on page 3

Keyboard input and navigation

The following features are available for keyboard input and navigation:

Keyboard input

You can use the keyboard instead of a mouse to operate the product.

Menu items and controls provide access keys that allow you to activate a control or select a menu item directly from the keyboard. These keys are self-documenting; the access keys are underlined on the control or menu where they appear.

Tip: To operate the default button in a window, press Enter. To operate any other button, move to the button and press the spacebar.

Keyboard focus

The position of the keyboard focus is highlighted, indicating which area of the window is active and where your keystrokes will have an effect.

Response time adjustments

On Windows systems, you can adjust response times through your control panel.

Keyboard shortcut keys

Use the keyboard to access all of the functions of the system administration clients.

In general, keyboard access conforms to standard Microsoft Windows guidelines. Mnemonics for functions such as menu items are underlined; you can access such functions by holding down the Alt key and pressing the underlined letter key. For example, you can open the **File** menu from the keyboard by holding down the Alt key and pressing F.

Keyboard access differs from standard Microsoft Windows guidelines in the following ways:

Access keys, tabbing, and tables

Access keys are provided only for buttons and menu items. Input components, like list boxes and combo boxes, have labels that allow you to access them and provide your input. Press Tab to reach fields that do not have a shortcut key combination.

Press the Tab key to move the cursor into a table. Press the Tab key again to move the cursor to the next cell within a table. To move out of the table to the next field, hold down the Ctrl key and press Tab. When the cursor is within a table, pressing Enter is not equivalent to clicking **OK** to close the window; you must move out of the table first.

If you want to edit a cell in a table that contains a combo box, press F2, use the down or up arrow key to move to an item, and press Enter to select it.

Combo boxes

Use the up and down arrow keys to move to an item, then press Enter to select it.

Menus

Press Alt and then Spacebar to open the **Program** menu from the left icon on the title bar of the System Administration Client window. When this menu is open, pressing the Alt key closes the menu.

Pressing Shift+F10 does not open pop-up menus. You can access pop-up menu functions from the **Selected** menu.

Tree views

You can expand or collapse a tree by pressing Enter or by using the Left and Right Arrow keys. Pressing the Asterisk (*) does not expand a tree selection. Pressing the Plus key or Minus key on the numeric key pad does not expand or collapse the tree. Typing characters or pressing Backspace while in the tree does not select an item.

If you have Java 2 Software Development Kit 1.4 on your system, then you can press a letter key and the next item in the tree that begins with that character is selected.

List boxes, check boxes, and radio buttons

In a list box, press the Down Arrow and Up Arrow keys to select an item. To select multiple sequential items, hold down the Shift key while pressing the Down or Up Arrow key.

If you have Java 2 Software Development Kit 1.4 on your system, you can press a letter key to select items within a list box, combination box, or table.

Within list boxes, the following actions have no effect:

- Pressing the Ctrl key with Page Up, Page Down, Home, or End
- Pressing a letter key (unless you have JRE 1.4 installed)
- Pressing Shift+F8

You can select individual radio buttons by pressing the Tab key and then the Spacebar, or by using the access keys. Arrow keys do not select radio buttons within a group.

Notebook tabs

Access keys are not provided for notebook tabs. Move the focus to a page tab using the Right and Left Arrow keys or the Tab key, or by pressing Ctrl+Page Down or Ctrl+Page Up.

Additional keystrokes

The following keys have no effect on text fields:

- Alt+Backspace
- Ctrl+Z
- Shift+Delete

Features for accessible display

The clients have a number of features that enhance the user interface and improve accessibility for users with low vision. These enhancements include support for high-contrast settings and customizable font properties.

High-contrast mode

In Windows systems, the clients support the high-contrast mode option that is provided by the operating system. This feature supports a higher contrast between background and foreground colors.

Font settings

In Windows systems, the client inherits the system settings that you specify for the color, size, and font for the text in menus and dialog windows. The client allows you to select the font for the document list.

Non-dependence on color

You do not need to distinguish between colors in order to use any function of this product.

Compatibility with assistive technologies

The clients are compatible with the JAWS screen reader application. The clients have the properties required for this accessibility application to make on-screen information available to visually impaired users.

Requirement: You must launch the JAWS screen reader using the **java** command instead of the **javaw** command; if you launch the screen reader with the **javaw** command, the screen reader does not work properly. The batch file that starts the system administration client uses the **javaw** command. Edit `cmadmin.bat` to change **javaw** to **java**.

Accessible documentation

Documentation for this product is available in accessible formats.

Documentation is available in an accessible Eclipse information center in HTML format. The HTML format allows users to view documentation according to the display preferences set in their browsers. It also allows the use of screen readers and other assistive technologies.

Documentation is also available in PDF format. You can convert the PDF files to HTML or text using free tools available from Adobe at access.adobe.com.

eClient accessibility

Through your browser, you can control font size and colors and use the browser's shortcut keys.

There are also special keyboard shortcut keys associated with the eClient viewer applet. The special keyboard shortcut keys are documented in the eClient online help. See the Accessibility page in the online help for more information.

Defining and configuring a library server

The library server, the key component of IBM Content Manager, stores, manages, and provides access control for objects stored on one or more resource managers.

You normally define your library server as part of the IBM Content Manager installation. The system administration client can connect to multiple library servers. If you need to connect to another library server, you must first define it and then configure it. You can change many of the configuration settings on the library server after it has been installed.

Important: Library servers do not communicate with one another. If you create an additional library server, it has no relationship to your existing one. Reasons for creating additional library servers include setting up a test environment and managing multiple distinct systems that are intentionally separated. You can manage multiple library servers from the same system administration client.

1. For a new library server, use the configuration wizard provided to create a library server database and initial configuration. For instructions about the configuration wizard, see the *Planning and Installing Your Content Management System* information.
2. Connect the system administration client to the library server. If the system administration client is installed on the same system as the new library server, no additional configuration is required. Skip to the next step. If the database is not on the same system, set up a connection to the remote library server.
3. Optional: Modify the library server configuration settings.
4. Assign resource managers to the library server.
 - UNIX or Windows resource manager
 - z/OS resource manager

Attention: You assign a default resource manager and collection to users when you create users. You assign a default resource manager and collection to an item type when you create the item type.

5. Define the languages that the library server will support for index information. The library server can support the index information (attributes and item types) for objects in one or more languages. You can define different languages on each of your library servers independently of the other library servers. Assign the languages that are used for index information to attributes and item types when you create attributes and item types.

“Login user exit scenarios” on page 17

Related reference

“Troubleshooting the library server” on page 600

Related information

Version 8.4.2 installation and configuration wizards

Library server

The library server, the key component of IBM Content Manager, enables you to define the information that you store in your library.

The library server is the key component of the IBM Content Manager system. It is called the library server because it performs the functions that a library catalog file in a real library performs; it is where you define the information that you store in your library. The library server stores, manages, and provides access control for objects stored on one or more resource managers. The library server processes requests (such as update or delete) from one or more clients and maintains data integrity between all of the components in the IBM Content Manager system.

The library server relies on a relational database management system (RDBMS), such as DB2 Universal Database™, to manage the content and perform parametric searches.

An IBM Content Manager system requires one library server, which can run on AIX®, Linux, Solaris, Windows, or z/OS. You can set up multiple library servers to meet your specific requirements.

Viewing or modifying the library server configuration

A library server configuration contains the parameters that are used to define the environment for the library server. Complete these steps to view or modify the library server configuration.

A library server configuration contains the parameters that are used to define the environment for the library server.

Tip: In the Features page of the Library Server Configuration window, you can set a timeout value for stopping a text indexing task that might be taking too long or has ended abnormally. Setting this timeout option allows the system to continue text indexing the next document. This timeout option is available only for library servers for Content Manager EE.

Restriction: You cannot modify the library server name.

1. Expand your library server in the tree view.
2. Expand **Library Server Parameters**.
3. Expand **Configurations**.
4. Right-click **Library Server Configuration** in the details pane and click **Properties** to open the Library Server Configuration window.
5. Click on the tab or tabs containing the settings you want to view or modify. See the related information for instructions about each tab:
 - Definition: configuration parameters, including logon information, system language, and trusted logon.
 - Features: configuration features, including text search and ACL user exit.
 - Defaults: configuration defaults, including default access list, storage options, and replication options.
 - Log and trace: log and trace information.
6. Click **OK** to save the information and close the window. Click **Apply** to save the information without closing the window.

Viewing or modifying the configuration parameters

Complete these steps to view or modify library server definition parameters.

Important: The following fields cannot be modified:

- The **Library Server name** field displays the name of the library server. If there are multiple library servers, the field also displays the ID of those library servers whose ID is not equal to 1. The local library server always has the ID of 1.
- The **Database type** field displays the type of library server database.
- The **Operating system** field displays the operating system on which the library server is running.

Attention: If you want to update the encryption key, wait for a period of low activity on the resource manager. It is possible for transactions to fail if they happen during the update. Also make sure that the resource manager is started before you click **Refresh encryption key**. If the resource manager is not running, then the keys will no longer match and the library server will not be able to connect to the resource manager.

On the Definition page in the library server configuration:

1. In the **Maximum logon attempts** field, type a value from 1 to 32767 as the maximum number of consecutive failed logon attempts a user can make before the user ID is locked. Set the value to 0 for no limit. If the user reaches the limit you set, the user is locked out of the system. A second user with administrative privileges must reset the first user's password before the first user can regain access to the system.
2. In the **Password duration** field, type a value from 1 to 32767 as the number of days that a password remains valid for all users of the library server. Set to 0 for no limit. The system will prompt users to change their passwords at the first logon attempt after a password expires. This value is only used when it is indicated to use the system default as the password expiration from a user's profile.
3. In the **Max users** field, leave the default value of 0.

Tip: To count the registered users, enter the following command at a DB2 command prompt:

```
select count(*) from icmstusers where userid not in
('ICMCONCT','ICMPUBLIC') and userkind=0
```

4. From the **Max user action** list, select the action to take if the maximum number of concurrent users is reached.
5. In the **Language** field, select a language name from the list. This language will be the default language for the library server.

Restriction: You must restart the system administration client for the language change to take effect.

6. Optional: Select the **Allow trusted logon** check box to allow IBM Content Manager users to have access to the library server without prompting for an additional password.

Important: You must include the privilege AllowTrustedLogon in the privilege set of the user ID that you want to allow for trusted logon. For system administrators, other than domain administrators, the password defined in the operating system is used for authentication against DB2 Universal Database.

Tip: The logon user exit is another way to bypass IBM Content Manager or IBM Information Integrator for Content federated password authentication. For example, the logon exit can be used to validate users against an LDAP

directory. See *Planning and Installing Your Content Management System* or *Planning and Installing Your Content Management System for z/OS*, as appropriate, for information about user exits.

7. Optional: Public access is disabled by default for performance reasons. If you select the **Enable public access** check box, all users are associated with the ICMPUBLIC user group and can access an item if an access control list associated with ICMPUBLIC is used for access to the item. If you clear the check box, the rules within the ACL that pair ICMPUBLIC with the privilege set are not applied. Other rules within the ACL remain valid. In general, do not enable public access.

Important: Performance is typically improved when this option is not enabled. However, disabling public access on a production system might result in user access difficulties if there are ACLs that rely on ICMPUBLIC. If you plan to change this setting on a production system, review all of your ACLs in advance. If you decide to make the change, you must complete the following tasks:

- a. If an ACL currently bound to an IBM Content Manager object contains ICMPUBLIC in one of its rules, create a new user group that includes all IBM Content Manager users.
- b. Update the ACL by removing the rule with ICMPUBLIC and adding a new rule with the newly created user group and the privilege set.

Tip: In previous versions of IBM Content Manager, public access was enabled by default. A library server that has been upgraded will retain the setting. If you do not notice any performance problems, there is no need to change it.

8. Click **Refresh encryption key** to generate a new encryption key. The library server uses an encryption key to generate a token. The token is used by the resource manager to retrieve or store objects. If you want to update the encryption key, you should wait for a period of low activity on the resource manager. It is possible for transactions to fail if they happen during the update. Also make sure that the resource manager is started before you click **Refresh encryption key**. If the resource manager is not running, the keys will no longer match and the library server cannot connect to the resource manager.

Recommendation: Periodically, you should refresh the key for security purposes. When you refresh, a new key is used to validate the token. In addition to following your organization's security guidelines, consider refreshing the key under the following circumstances:

- After installation
 - After an upgrade
 - When the encryption key has been compromised
9. Click **OK** to save changes and exit or **Apply** to save changes and continue working.

Related tasks

“Resetting user passwords” on page 461

Viewing or modifying the configuration features

Complete these steps to enable, view, or modify library server feature parameters.

On the Features page in the library server configuration:

1. If you want attributes to be text searchable, select the **Enable Text Search** check box to enable text searching. For Content Manager EE, enter the user ID and password.

Important: For Content Manager EE, unless DB2 Universal Database is set up to start text search automatically, you must restart text search each time you restart the system. At a DB2 command prompt, enter:

```
db2text start
```

2. For Content Manager EE, if you want to set a timeout value for stopping a text indexing update task that might be taking too long or has ended abnormally, select **Enable text indexing timeout**.
3. For Content Manager EE, if you selected **Enable text indexing timeout**, select a **Text indexing timeout** value that indicates the maximum amount of time you want the text indexing task to spend on a particular document before continuing to the next document. The default timeout value is 300 seconds.
4. To enable your system for IBM FileNet® Records Manager, select **Enable Records Management**. If you enable IBM FileNet Records Manager, you cannot disable it at a later time.

If you already have IBM Records Manager on your system, the IBM Records Manager option displays as enabled. If you do not already have IBM Records Manager on your system, the IBM Records Manager option is disabled because you cannot enable IBM Records Manager by using this method.

Restriction: IBM Records Manager is not supported by a library server on z/OS.

5. To reset the event monitor, click **Reset event monitor active flag**.
6. To enable your system for event subscriptions, select **Enable Event Subscriptions**.
7. If you created an exit routine for access control, select **Enable ACL user exit** to enable it. The exit routine might determine whether a user has the authority to perform the requested function on a particular item or view.
8. Optional: To disable the dynamic generation and display of component, index, and large object (LOB) table space information from the database manager tables, select the **Disable dynamic table space information** check box. Although you can assign table, index, and LOB table spaces in the system administration client for Content Manager EE and table table spaces in Content Manager for z/OS, table spaces can be changed by the database administrator during customization of the database. As a result, the table space information that is displayed when you are creating or modifying components or indexes might not be correct. If the **Disable dynamic table space information** check box is selected, then the library server returns the current default table spaces that were set when the item type or component was created or modified. If the **Disable dynamic table space information** check box is not selected, then the library server retrieves this information for the system administration client and the information is always correct. However, as the number of components increases, this retrieve action can affect the performance of the system administration client and library server.

Restriction: Currently, the system administration client can display dynamic table space information for the index table space only when you are viewing the index properties and can display dynamic table space information for the table space only in the Set Table Spaces window.

Recommendation: In most cases, you can leave the **Disable dynamic table space information** check box at the default setting. You might want to disable the dynamic display of table space information if you are experiencing a performance problem with the system administration client.

9. Review the status message for the access control list (ACL) mode. This message shows the mode that the library server is using to insert ACL rules into the ICMSTCompiledACL table in the library server database. With the time-optimized ACL mode, the default mode, all possible combinations of ACL rules, user groups, and privileges are generated by the library server and stored in the ICMSTCompiledACL table. With the space-optimized ACL mode, the user groups are not expanded and only one instance of the combination of the ACL and user group is stored in the ICMSTCompiledACL table.
 10. Click **OK** to save changes and exit or **Apply** to save changes and continue working.
- “Changing the ACL optimization mode” on page 25

Viewing or modifying the configuration defaults

Complete these steps to view or modify library server default parameters.

On the Defaults page in the library server configuration:

1. Specify the default storage options:
 - a. In the **Get default resource manager from** field, select a method for assigning a default resource manager on which to store an object. Select **User** to use the default resource manager assigned in users' profiles. Select **Item type** to use the default resource manager specified for item types.
 - b. In the **Get default collection from** field, select a method for assigning an object to a default collection. A collection identifies a group of related objects with similar storage management criteria. Select **User** to use the default collection assigned in users' profiles. Select **Item type** to use the default collection specified for item types.
2. Specify the default options for replication:
 - a. In the **Interval to check server availability** field, enter the amount of time in seconds that the library server checks the availability of the resource manager. The default is 60 seconds.
 - b. In the **Server timeout threshold** field, enter the amount of time in seconds after which the library server considers a resource manager unavailable if it does not receive a response. The default is 15 seconds.
3. Click **OK** to save changes and exit or **Apply** to save changes and continue working.

Viewing or modifying log and trace information

Complete these steps to enable system administration event logging, or to view or modify library server log and trace information.

Logging events is important for different reasons. For example, it can serve security and audit purposes by helping you determine which users made certain changes on the system. On the Log and Trace page in the library server configuration:

1. To enable logging of system administration events, select the **Allow system administrator event logging** check box. System administration events include creating users, access control lists, and privileges. See the library server event logging table for examples of the data that you might see in the event log.

2. Specify what level of trace will be added to the log file. You can select multiple trace levels by selecting more than one check box.
 - **Basic trace** logs entry and exit from all stored procedures and lower level functions.
 - **Detailed trace** logs execution flow through the stored procedures.
 - **Data trace** logs input parameters and large quantities of data through the execution.
 - **Performance trace** logs elapsed execution time (in milliseconds) for each stored procedure.
3. In the **Trace file name** field, specify the name for the trace file. The directory that you specify in the field must exist and you must have write access to create the trace file. If your library server is local, you can click **Browse** to select a file name from your file system.
4. Click **OK** to save changes and exit or **Apply** to save changes and continue working.

Related concepts

“Event logging” on page 414

Related reference

“ICM library server event table log” on page 418

Single sign-on options

The IBM Content Manager single sign-on options enable you to log on only once for multiple applications.

With single sign-on, users can log on once to either a website or desktop system and not have to log on to different applications from the same website or desktop system. IBM Content Manager provides two types of single sign-on capabilities for two environments (web and desktop):

- “Single sign-on through WebSphere security”

Single sign-on through WebSphere security

Use this single sign-on function in a WebSphere® Application Server environment.

You can use this function with Web applications in a WebSphere Application Server environment to take advantage of WebSphere security and its single sign-on capability.

When a user requests a resource from a server, the server collects the access control lists (ACLs) associated with that resource and evaluates them. If the server evaluation of the ACLs requires identification of the user, the server requests client authentication in the form of either a name and password pair or a digital certificate presented according to the SSL protocol.

After the server establishes the user's identity, optionally including user or group information stored in an LDAP directory, it continues its evaluation of the ACLs. Then the server authorizes or denies access to the requested information according to the user's access privileges.

To enable this authentication mechanism, complete the following setup steps in the system administration client:

1. In the Library Server Configuration window, select **Allow Trusted Logon**.
2. Create a privilege set that contains the TrustedLogon privilege.

3. Create each IBM Content Manager user ID with the TrustedLogon privilege set. These users do not need to be operating system users. They can be IBM Content Manager users only. In the case where the users are not operating system users, you must set up a connection user ID either during the installation or from the server configuration utility. The connection user ID must be an operating system user ID that has permission to establish the connection to the database.

Requirement: Web applications must use the `connectWithCredential()` method instead of the `connect()` method.

Creating a language definition

Complete these steps to create language definitions for your library server configuration.

You can provide translations for numerous **Display Name** fields in IBM Content Manager if you first create a language definition. A language definition consists of a language code and a language name. A language definition does not determine the language in which the system administration client is displayed.

Tip: To change the language for a library server, modify the library server's configuration parameters. To change the language of the system administration client, install the system administration client in that language.

To create a language definition:

1. Expand your library server in the tree view.
2. Expand **Library Server Parameters**.
3. Right-click **Language Definitions** and click **New** to open the New Language Definition window.
4. In the **Language** field, type a descriptive language name. The language name must be between 1 and 32 alphanumeric characters and can contain spaces.
5. In the **Language Code** field, type or select the code from the list.
6. Click **OK** to save the language definition. Click **Apply** to save the language definition and keep the window open to create another language definition.

Language definition

Creating language definitions for your library server configuration enables you to provide translated display names for users who speak different languages.

Several windows in the system administration client have **Display name** fields that have a **Translate** button next to them. (For an example, see the properties for an item type or attribute.) If you have to set up your system for users who speak different languages, then you need to define these languages to the library server and provide translated display names.

You must specify a language code if you plan on translating text from one language to another. A language code is a three-character code that can be used to display attributes or item types in multiple national languages. When you specify a language code, you also need to enter the equivalent word in that language.

After you define the language codes that your system recognizes, you use the **Translate** button to put in the translated terms, changing how that term is viewed by the user of the client application. For example, if you have an attribute that you

named Street and have Spanish as one of the languages defined to your library server, you can click the **Translate** button and type *Calle*. So, when users who use a Spanish version of the client application need to give a value for the attribute Street, they will see *Calle* for the attribute instead.

In order for a translated name to appear for an attribute, you must provide the translation when you create or update the attribute. You should define the attribute in every language that the attribute is used on your system. If an attribute displays in a language that is different from the language defined on a machine, an asterisk (*) displays before the attribute name.

Related concepts

“Display name” on page 107

“Attributes” on page 148

“Item type” on page 156

Language codes

Refer to this list for the correct language code to specify when creating a language definition.

A language code must be one of the following three-character codes:

Table 1. Language codes available in IBM Content Manager

Language	Language code
Afrikaans	AFR
Albanian	SQI
Arabic	ARA
Australian English	ENA
Bulgarian	BEL
Byelorussian	BGR
Catalan	CAT
Chinese, Simplified	CHS
Chinese, Traditional	CHT
Croatian	HRV
Czech	CSY
Danish	DAN
Dutch	NLD
Dutch, Belgian	NLB
English, United Kingdom	ENG
English, US	ENU
English, uppercase	ENP
Finnish	FIN
French	FRA
French, Belgian	FRB
French, Canadian	FRC
French, Swiss	FRS
German	DEU

Table 1. Language codes available in IBM Content Manager (continued)

Language	Language code
German, Swiss	DES
Greek	ELL
Hebrew	HEB
Hungarian	HUN
Irish Gaelic	GAE
Icelandic	ISL
Italian	ITA
Italian, Swiss	ITS
Japanese	JPN
Korean	KOR
Lithuanian	LTH
Macedonian	MKD
Norwegian Bokmal	NOR
Norwegian Nynorsk	NON
Polish	PLK
Portuguese	PTG
Portuguese, Brazilian	PTB
Rhaeto-Romanic	RMS
Romanian	ROM
Russian	RUS
Serbian, Cyrillic	SRB
Serbian, Latin	SRL
Slovakian	SKY
Slovenian	SLO
Spanish	ESP
Swedish	SVE
Thai	THA
Turkish	TRK
Ukrainian	UKR
Urdu	URD

Additional language definitions

You can create additional language definitions for languages that are not currently included in the language codes selection list.

There is a list of approximately 50 three-letter language codes that you can use to define a new language in the New Language Definition window of the system administration client. You can type any three-letter language code, as long as all the three letters belong to the set A-Z (uppercase) and 0-9. The New Language Definition window still presents the list of approximately 50 language codes that you can select from, but it now also allows you to enter any three unique letters or numbers that you want.

Restriction: The 3-letter language code must be unique in an IBM Content Manager system. If you try to enter a language code that already exists, the **OK** button is not enabled.

The IBM Content Manager client applications are not translated into all languages. If you create a language that does not map to a language into which the client application is translated, the client application still allows you to select the language that you want. The attributes, item types, and other similar objects are displayed with the descriptive names that were saved with the selected language translation, however, the client application itself appears in English. In this situation, ensure that you install the English language resources on your client workstations, along with the other language resources that you want. Otherwise, there might be unpredictable results. Check the documentation for your client for more specific information about how to select languages.

Attention: If you want to use language-specific characters in your descriptive names or attribute values, ensure that you install your IBM Content Manager library server database by using either a code page that supports your desired characters or by using a Unicode code page. Entering language-specific characters in a database that has no code page conversion for that language results in a loss of data stored in the IBM Content Manager database.

The following examples describe language-specific IBM Content Manager systems.

Single code page, single language

Create an IBM Content Manager database by using Windows code page 1258 (Vietnamese). Because this code page only supports Vietnamese and English, you only create one additional language on your library server, in addition to the default English. The language code for Vietnamese is VIE.

Single code page, multiple languages

Create an IBM Content Manager database by using the ISO-8859-4 code page, which is designed for north European languages. In this case, you can create more than one language, because the code page is designed for more than one language. For example, you might want to use ESG for Greenlandic, LIT for Lithuanian, and LAV for Latvian, in addition to the default English language.

Unicode code page, multiple languages

Create an IBM Content Manager database by using Unicode code page UTF-8, which is designed to support many languages. In this case, you can create many different languages by using appropriate three letter language codes.

Viewing or modifying a language definition

Complete these steps to view or modify an existing language definition in your library server configuration.

You can modify a language name, but you cannot modify the language code of an existing language definition. To view or modify an existing language definition:

1. Expand your library server in the system administration tree.
2. Expand **Library Server Parameters** in the system administration tree.
3. Click **Language Definitions** to display all the language definitions in the right pane.
4. Right-click the language definition you want to view or modify and click **Properties** to display the Properties window.

5. To change the name of the language definition, type a new descriptive language name in the **Language** field. The language name must be between 1 and 32 alphanumeric characters and can contain spaces.
6. Click **OK** to save the information and close the window.

Deleting a language definition

Complete these steps to delete a language definition from your library server configuration.

If you delete a language definition, any existing translations for that language are deleted also.

To delete a language definition:

1. Expand your library server in the system administration tree.
2. Expand **Library Server Parameters**.
3. Click **Language Definitions** to display all the language definitions in the right pane.
4. Right-click the language definition that you want to delete and select **Delete**.
5. Click **Yes** to confirm the deletion.

Changing the library server and system administrator password to the resource manager

Complete these steps to change the password that the system administration client and library server use to access the resource manager.

To change the password that the system administration client and library server use to access the resource manager, complete the following steps. It is important that the password is changed in both places by following the indicated order in this procedure.

Attention: Performing these tasks does not affect the database user ID and password that are used by the resource manager to access the database.

1. Log on to the system administration client.
2. Expand your library server in the tree view.
3. Expand **Resource Managers**.
4. **For all operating systems except z/OS:** Expand the resource manager that you want to modify.
5. **For all operating systems except z/OS:** Change the password stored on the resource manager:
 - a. Click **Server Definitions**. Right-click the resource manager server in the right pane and select **Properties**. The Server Definition Properties window opens.
 - b. Change the password in the **Password** field.
 - c. Click **OK** to save the new password.
6. Change the password stored on the library server:
 - a. Right-click your resource manager in the left pane and select **Properties**. The Resource Manager Properties window opens.
 - b. Change the password in the **Password** field.
 - c. Click **OK** to save the new password.

Related reference

"System accounts and passwords" on page 661

Login user exit scenarios

You can log in to the library server by using login user exit routines.

The following scenarios depend on whether you are an IBM Content Manager administrator or nonadministrative user who is logging in to the library server. In addition, there are scenarios when **Allow trusted logon** is selected for user authentication.

The following list defines the variables in these scenarios:

Type of IBM Content Manager user

IBM Content Manager administrator

This user is defined in IBM Content Manager and in the operating system. In addition, this user must be part of the database administrator group. For example, the default is ICMADMIN.

Non-administrative user

This user is defined only in IBM Content Manager, that is the user is not defined in the operating system.

Server connection

SERVERREPTYPE

SERVERREPTYPE is a parameter in the cmbicmsrvs.ini file. This file resides on the same workstation as your client. One of the following values indicates how the client connects to the IBM Content Manager library server.

DB2 Tells the API to use the user ID and password that is entered in the login window to connect to DB2 on the server. If the DB2 connection fails, the shared connection ID and password are used in a second attempt to connect.

DB2CON

Tells the API to use the shared client ID and password on the first connection. Therefore, the user is a nonadministrative user and can connect only through the shared connection ID.

Login User Exit

The action that is used by the IBM Content Manager library server to authenticate a user varies depending on whether a login user exit routine is configured.

Trusted logon

Trusted logon allows IBM Content Manager users to have access to the library server without prompting for an additional password.

The following scenarios apply to a configuration where trusted logon is not enabled.

Table 2. Logon scenarios. IBM Content Manager Version 8 logon scenarios. SERVERREPTYPE is DB2

IBM Content Manager user type	Is a logon user exit routine in place?	API logic	Server logic
Administrator	N	The API connects to the database using the user ID and password entered on the login window. Login succeeds.	<p>DB2 allows the connection because this user has authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID is the same as the IBM Content Manager user ID. It does not perform password authentication because that analysis was already done by DB2.</p>
Administrator	Y	The API connects to the database using the user ID and password entered on the login window. Login succeeds.	<p>DB2 allows the connection because this ID is the administrator who has authority to connect to DB2.</p> <p>The user exit is loaded.</p> <p>The user logs on successfully because either of the following conditions are true:</p> <ul style="list-style-type: none"> • The user exit routine authenticated the user thus bypassing the IBM Content Manager password authentication. • The user exit routine did not authenticate the user, but because the password authentication was already performed by DB2, the user logs on successfully.
IBM Content Manager user (nonadministrator)	N	<ul style="list-style-type: none"> • The API connects to the database with the user ID and password entered on the login window and fails. • The API connects to the database with the shared connection ID and password and login succeeds. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user ID are different. IBM Content Manager uses its own logic to authenticate the IBM Content Manager user password.</p>

Table 2. Logon scenarios (continued). IBM Content Manager Version 8 logon scenarios. SERVERREPTYPE is DB2

IBM Content Manager user type	Is a logon user exit routine in place?	API logic	Server logic
IBM Content Manager user (nonadministrator)	Y	<ul style="list-style-type: none"> The API connects to the database with the user ID and password entered on the login window and fails. The API connects to the database with the shared connection ID and password and login succeeds. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user IDs are different. IBM Content Manager also confirms that a login user exit is in place and invokes the login user exit to authenticate the IBM Content Manager user ID. If the exit fails to authenticate the user, IBM Content Manager performs its own authentication by using the user's IBM Content Manager password.</p>
IBM Content Manager user with the privilege SystemSuperDomainAdmin and with a null password in IBM Content Manager (nonadministrator)	N	<ul style="list-style-type: none"> The API connects to the database with the user ID and password entered on the login window and fails. The API connects to the database with the shared connection ID and password and login succeeds. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user IDs are different. IBM Content Manager password authentication fails with exception ICM7172: The password provided is invalid for this user or it is NULL.</p> <p>Users with the administrative privilege SystemSuperDomainAdmin are required to have a password to log on to IBM Content Manager.</p>

Table 2. Logon scenarios (continued). IBM Content Manager Version 8 logon scenarios. SERVERREPTYPE is DB2

IBM Content Manager user type	Is a logon user exit routine in place?	API logic	Server logic
IBM Content Manager user with the privilege SystemSuperDomainAdmin and with a null password in IBM Content Manager (nonadministrator)	Y	<ul style="list-style-type: none"> The API connects to the database with the user ID and password entered on the login window and fails. The API connects to the database with the shared connection ID and password and login succeeds. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user IDs are different. IBM Content Manager also confirms that a login user exit routine is in place and invokes it to authenticate the IBM Content Manager user ID.</p> <p>If the user exit routine fails to authenticate the user, IBM Content Manager performs its own password authentication by using the user's IBM Content Manager password. IBM Content Manager password authentication fails with the exception ICM7172: The password provided is invalid for this user or it is NULL.</p>

The following scenarios describe when the SERVERTYPE parameter is set to DB2CON.

Table 3. Logon scenarios. Various IBM Content Manager Version 8 login scenarios. SERVERREPTYPE is DB2CON

IBM Content Manager user type	Is a logon user exit routine in place?	API logic	Server logic
Administrator	N	<ul style="list-style-type: none"> The API connects to the database with the shared connection user ID because the SERVERREPTYPE is DB2CON. The API catches the 7271 login error and connects again to the database using the IBM Content Manager user ID and password entered on the logon window. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager does not allow IBM Content Manager administrators to log in with the shared connection ID and returns an error code of 7271. On the second login call, IBM Content Manager confirms that the connection ID is the same as the IBM Content Manager user ID and bypasses password authentication.</p>

Table 3. Logon scenarios (continued). Various IBM Content Manager Version 8 login scenarios. SERVERREPTYPE is DB2CON

IBM Content Manager user type	Is a logon user exit routine in place?	API logic	Server logic
Administrator	Y	<ul style="list-style-type: none"> The API connects to the database with the shared connection user ID because the SERVERREPTYPE is DB2CON. The API catches the 7271 login error and connects again to the database using the IBM Content Manager user ID and password entered on the logon window. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager does not allow IBM Content Manager administrators to log in with the shared connection ID, and returns an error code of 7271. On the second login call, IBM Content Manager confirms that the connection ID is the same as the IBM Content Manager user ID and bypasses password authentication, regardless of the presence of the login user exit routine.</p>
IBM Content Manager user (nonadministrator)	N	<p>The API connects to the database with the shared connection user ID because the SERVERREPTYPE is DB2CON.</p> <p>Tip: The initial attempt with the user ID and password from the logon window is skipped.</p>	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user ID are different, and uses its own logic to authenticate the IBM Content Manager user password.</p>
IBM Content Manager user (nonadministrator)	Y	<p>The API connects to the database with the shared connection user ID because the SERVERREPTYPE is DB2CON.</p> <p>Tip: The initial attempt with the user ID and password from the login window is skipped.</p>	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user ID are different. IBM Content Manager also confirms that a login user exit is in place and invokes it to authenticate the IBM Content Manager user ID. If the exit fails to authenticate the user, IBM Content Manager performs its own authentication by using the user's IBM Content Manager password.</p>

You can bypass password authentication for any IBM Content Manager user by configuring your system to allow trusted logon:

1. Enable the Shared Connection ID for trusted log on:
 - a. Open the system administration client.
 - b. Click **Tools > Manage Database Connection ID > Change Shared Database Connection ID and Password**.
 - c. Clear the check box **Password is required for all users**.

By default, it is disabled.

2. Enable the library server configuration flag Allow trusted logon. From the system administration client, click **Library Server Parameters > Configurations > Library Server Configuration**. Ensure that Allow trusted logon is selected.
3. Include the AllowTrustedLogon privilege in the IBM Content Manager users' privilege set. To verify, go to the system administration client and open the user's properties panel. Ensure that the privilege set for the user contains the AllowTrustedLogon privilege.

If you are using the trusted logon configuration, the following login scenarios apply. The SERVERTYPE parameter for all scenarios can be DB2 or DB2CON.

Table 4. Logon Scenarios. IBM Content Manager Version 8 login scenarios with trusted logon enabled. SERVERREPTYPE is DB2 or DB2CON

IBM Content Manager user type	Is a logon user exit routine in place?	API logic	Server logic
Administrator	Y or N	The API connects to the database by using the user ID and password entered on the login window. Login succeeds.	DB2 allows the connection because this user has authority to connect to DB2. IBM Content Manager confirms that the connection ID is the same as the IBM Content Manager user ID. It does not perform password authentication because that analysis has already been done by DB2.
IBM Content Manager user (nonadministrator)	N	<ul style="list-style-type: none"> • The API connects to the database with the user ID and password entered on the login window and fails. • The API connects to the database with the shared connection ID and password and login succeeds. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user IDs are different. If all trusted log on is enabled, IBM Content Manager bypasses any password authentication.</p>
IBM Content Manager user (nonadministrator)	Y	<ul style="list-style-type: none"> • The API connects to the database with the user ID and password entered on the login window and fails. • The API connects to the database with the shared connection ID and password and login succeeds. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user IDs are different. IBM Content Manager also confirms that a login user exit is in place and invokes it to authenticate the IBM Content Manager user ID.</p> <p>If the user exit routine authenticates the user, log on is successful. If the user exit routine fails to authenticate the user, but trusted log on is enabled, log on is successful.</p>

Table 4. Logon Scenarios (continued). IBM Content Manager Version 8 login scenarios with trusted logon enabled. SERVERREPTYPE is DB2 or DB2CON

IBM Content Manager user type	Is a logon user exit routine in place?	API logic	Server logic
IBM Content Manager user with a null password and the privilege SystemSuperDomainAdmin (nonadministrator)	N	<ul style="list-style-type: none"> The API connects to the database with the user ID and password entered on the login window and fails. The API connects to the database with the shared connection ID and password and login succeeds. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user IDs are different. IBM Content Manager password authentication fails with exception ICM7172: The password provided is invalid for this user or it is NULL.</p> <p>Users with the administrative privilege SystemSuperDomainAdmin are required to have a password to log on to IBM Content Manager. Trusted log on does not apply to users with a null password and the IBM Content Manager administrative privilege.</p>

Table 4. Logon Scenarios (continued). IBM Content Manager Version 8 login scenarios with trusted logon enabled. SERVERREPTYPE is DB2 or DB2CON

IBM Content Manager user type	Is a logon user exit routine in place?	API logic	Server logic
IBM Content Manager user with a null password and the privilege SystemSuperDomainAdmin (nonadministrator)	Y	<ul style="list-style-type: none"> The API connects to the database with the user ID and password entered on the login window and fails. The API connects to the database with the shared connection ID and password and login succeeds. 	<p>DB2 allows the connection because the shared connection ID has the authority to connect to DB2.</p> <p>IBM Content Manager confirms that the connection ID and IBM Content Manager user IDs are different. IBM Content Manager also confirms that a login user exit routine is in place and invokes it to authenticate the IBM Content Manager user ID.</p> <p>If the user exit routine fails to authenticate the user, IBM Content Manager performs its own password authentication by using the user's IBM Content Manager password. IBM Content Manager password authentication fails with the exception ICM7172: The password provided is invalid for this user or it is NULL.</p> <p>Users with the administrative privilege SystemSuperDomainAdmin are required to have a password to log on to IBM Content Manager. Trusted log on does not apply to users with a null password and the IBM Content Manager administrative privilege.</p>

“Verify whether a user exit routine is being invoked”

“Checking which user ID is being used as the shared connection ID” on page 25

Verify whether a user exit routine is being invoked

You can verify whether a user exit routine is being invoked by looking in the SYSPRINT job.

In the sample source code, if a user exit routine is called the following printf function is included in the SYSPRINT job:

Call RACROUTE assembler code here

Tip: You can also add printf functions specific to your configuration that display in the SYSPRINT job to verify that a user exit routine was invoked.

Checking which user ID is being used as the shared connection ID

You can verify which user ID is being used as the shared connection ID by setting your trace level to 15.

To verify which user ID is being used:

1. Set your trace level to 15.
2. Open your library server log (the default is ICMSERVER.log).
3. Look for the following:

```
ICMPLSLG ICMLOGON 00756 02/01 06:02:58.935 GMT ;01060258319384 ? ICMADMIN Input
UserID      <ICMADMIN>
DB2UserID   <ICMADMIN>
Language    <ENU>
Application  <ICM Connector>
```

The ID that is listed for DB2UserID is the user ID that is used for the connection to the database.

Changing the ACL optimization mode

You can change the access control list (ACL) optimization mode to affect how data is added to the ICMSTCompiledACL table. The optimization modes determine how the ACL data and the ICMSTCompiledACL table affect some administrative and runtime operations.

Before you change the ACL optimization mode, stop all running processes for your content management system, including all library server and resource manager processes. Changing the ACL optimization mode results in a regeneration of the ICMSTCompiledACL table, and this regeneration could consume a large amount of system resources. Do these steps only as a maintenance task in a system that is offline.

Important: In a content management system with many combinations of ACLs, users, and user groups, a change from the space-optimized ACL mode to the time-optimized ACL mode could result in thousands or even millions of rows being added to the ICMSTCompiledACL table. If you plan to make this type of change, you might need additional disk space on the database.

A change to the ACL optimization mode changes the way that ACL data and user data is added to the ICMSTCompiledACL table. The time-optimized ACL mode, the default mode, adds all possible combinations of ACL rules, user groups, and privileges to the table. The space-optimized ACL mode adds only one combination of the ACL and user group to the table. Change the ACL optimization mode only after careful consideration of the needs and structure of your content management system.

Important: Evaluate any change with performance benchmark testing on a test system before you change your production system.

To change the ACL optimization mode:

1. For operating systems based on UNIX such as AIX and Linux: To use the interactive mode to run the **cmcfglsl** command in this procedure, set and export the following environment variables as the root user:

Option	Description
DB2	<p>\$IBMCMROOT, \$instOwner, \$dbType, and \$INSTHOME</p> <p>For example:</p> <pre>IBMCMROOT=/opt/IBM/db2cmv8 instOwner=icmadmin dbType=DB2 INSTHOME=/home/db2inst1 export IBMCMROOT export instOwner export dbType export INSTHOME</pre>
Oracle	<p>\$IBMCMROOT, \$instOwner, \$dbType, \$ORACLE_HOME</p> <p>For example:</p> <pre>IBMCMROOT=/opt/IBM/db2cmv8 instOwner=ibmcadm dbType=ORACLE ORACLE_HOME=/usr/oracle/product/11.2.0 export IBMCMROOT export instOwner export dbType export ORACLE_HOME</pre>

- Log on to the database with a user ID that has administrative authority. For example, log on to the database with the default library server database administration ID, icmadmin.
- Enter one of the following commands to change the ACL optimization mode in the ICMSTSysControl table. For the DB2 for z/OS database, use SPUFI or a DB2 command prompt to enter the command.

Option	Description
To change the mode from the time-optimization ACL mode to the space-optimization ACL mode:	<p>Enter the following command on a single line:</p> <pre>update icmstsyscontrol set systemflag2 = systemflag2 + 16384 where Mod((systemflag2+2147483648), 16384*2) < 16384</pre> <p>Restriction: To use the space-optimization ACL mode with DB2, you must set the DB2_EXTENDED_OPTIMIZATION environment variable as follows to improve the speed of the query operation:</p> <pre>db2set DB2_EXTENDED_OPTIMIZATION=GY_DELAY_EXPAND</pre> <p>Enable the new environment variable by stopping the database with the db2stop command and then starting the database with the db2start command.</p>
To change the mode from the space-optimization ACL mode to the time-optimization ACL mode:	<p>Enter the following command on a single line:</p> <pre>update icmstsyscontrol set systemflag2 = systemflag2 - 16384 where Mod((systemflag2+2147483648), 16384*2) >= 16384</pre>

These commands change the value of bit 14 of the systemflag2 column of the ICMSTSysControl table.

- Enter the following command to regenerate the ICMSTCompiledACL table, based on the type of database that you are using.

Option	Description
DB2 for Linux, UNIX and Windows or Oracle	<p>Enter the following command, where <i>debug_level</i> is the debug logging level and <i>log_file</i> is the path of the log file to contain these messages. The <i>debug_level</i> and <i>log_file</i> values are optional, but can help you troubleshoot any problems with the cmcfiglsi command.</p> <pre>cmcfiglsi -t cac1 -d <i>debug_level</i> -l <i>log_file</i></pre> <p>For example:</p> <pre>cmcfiglsi -t cac1 -d 3 -l logfile /tmp/cac1.log</pre>
DB2 for z/OS	<p>Resubmit the following jobs:</p> <pre>icmmcac1.icmins1 cmcfiglsi -t comtypes</pre>

These actions also regenerate the ICMSTCompiledPerm table, but no changes are made to the table as a result of this procedure.

“Access control list optimization modes for the entries in the ICMSTCompiledACL table”

“Running performance testing for the ACL optimization modes” on page 29

Access control list optimization modes for the entries in the ICMSTCompiledACL table

The access control list optimization modes affect how data is added to the ICMSTCompiledACL table. You can choose the best way to store this data in your content management system, whether the size of the table or the time used to access the data in the table is of primary importance.

The ICMSTCompiledACL table is library server database table that contains the compiled access control list (ACL) information. Data can be stored to this table by using two modes that affect the way ACL and user data is added:

Time-optimized ACL mode

A mode where all possible combinations of ACL rules, user groups, and privileges are generated by the library server and stored in the ICMSTCompiledACL table in the library server database. Because all of the combinations are stored in this table, this table is used during runtime operations to perform privilege and ACL checking. A simple look-up action checks for the required privileges for a user with the given ACL.

Space-optimized ACL mode

A mode where the user groups are not expanded into individual users to generate the possible combinations with the ACL rules and privileges. Only one instance of the combination of the ACL and user group is stored in the ICMSTCompiledACL table. Because all combinations are not stored in the table, the ACL checking operation must complete additional tasks during runtime operations. These tasks include expanding the user group and checking if the user has the correct ACL and privileges to do the selected task.

How to evaluate which mode is best for your content management system

The option to select between the time-optimized ACL mode and the space-optimized ACL mode is a new feature for Version 8.4.3. The time-optimized ACL mode is the default mode. In earlier versions, only the time-optimized ACL mode is available.

A change from one ACL optimization mode to another is a process that you must carefully consider. Ideally, this change is a process that is only performed one time on your production content management system based on a thorough examination of the specific requirements of that system. You should also consider the following information about a change to the ACL optimization mode:

- The change between modes requires a regeneration of the ICMSTCompiledACL table. This regeneration might consume a large amount of system resources and should be done only as a maintenance task when the system is offline.
- If you change from a space-optimized ACL mode to a time-optimized ACL mode (the default mode), the size of the ICMSTCompiledACL table can increase significantly. Additional disk space might be required to accommodate the addition of many rows, possibly thousands or millions of rows, to the ICMSTCompiledACL table.
- If you are considering a change from one ACL optimization mode to another, you should test the performance for each mode on a test system before deploying the change into your production environment.

For most content management systems, allowing the setting to remain in the default time-optimized mode is the recommended action. This mode has the least impact on runtime operations during ACL checking.

A content management system that is likely to benefit from the use of the space-optimized ACL mode is a system that meets the following characteristics:

- It uses a collaborative content management model. In this model, individual users can create and manage their own documents and can collaborate with other users to interactively create and manage documents.
- It has many users, large user groups, and many ACL rules to manage the user collaboration.
- It regularly adds more users, user groups, and ACLs to the system as more documents are created.

If a collaborative content management system with these characteristics is set up to use the time-optimized mode, the large user groups and multiple user ACL rules would result in an ICMSTCompiledACL table that could be many millions of rows. For example, a collaborative content management system might be designed with many user groups that contain 1000 members each. Each document in this system might have several ACLs created for it. When one ACL is created for one of these user groups, 1000 insert actions must be performed in the ICMSTCompiledACL table. For an ACL that has several rules for multiple user groups, the number of rows inserted for a single ACL might be several thousand rows. If every document has several ACLs, then the ICMSTCompiledACL table could grow rapidly.

A table of that size might have performance problems during routine administrative tasks. These routine tasks might include creating user ACLs and adding, deleting, and moving users and user groups.

Tip: Performance problems related to the size of database tables are affected by the hardware capabilities and available resources in an individual content management system. However, a system where the size of the ICMSTCompiledACL table is approximately 10 million rows and will grow larger might benefit from changing from the time-optimized ACL mode to the space-optimized ACL mode. Also, if administrative tasks such as the creation of user ACLs become much slower, then you might want to consider whether the space-optimized ACL mode is right for your system.

If this example collaborative content management system uses the space-optimized ACL mode for the ICMSTCompiledACL table instead, this choice results in a table with significantly fewer rows, approximately equal to the number of ACLs plus rows for users who have the ItemSuperAccess privilege. The result might be better performance during routine maintenance tasks for ACLs, users, and user groups.

However, the use of the space-optimized ACL mode might affect the performance of query and retrieve actions because the additional ACL checking for users is done at run time. The degree to which the query and retrieve performance is affected depends on factors such as the number and size of user groups that are associated with ACL rules. For this reason, performance testing of both modes on a test system is recommended before you change the mode on your production system.

Running performance testing for the ACL optimization modes

Set up a test system to determine which ACL optimization mode for the ICMSTCompiledACL table yields the best performance results for your content management system.

The access control list (ACL) optimization modes determine how data is stored to the ICMSTCompiledACL library server table. Before you change from one ACL optimization mode to another in your production system, test the performance for each mode on a test system.

To set up a test system and perform benchmark testing for each mode:

1. Create a test system that closely resembles your production system. Set up the test system to have a comparable number of users, user groups, and ACLs and a similar data model for item types, privileges, versioning, and distribution of ACL assignments to items.
2. Gather performance data such as response time, processor (CPU) usage, and disk I/O for this test system to get a baseline measurement of the performance data. The testing should focus on query, retrieve, and document routing operations, and folder operations if applicable. The Information Roadmap for IBM Content Manager contains resources in the "Tuning" section to help you gather and analyze performance data.
3. Use the procedure to change the ACL optimization mode to change the mode on the test system.
4. Gather performance data again for the test system with the changed ACL optimization mode. As with the previous test, the performance data that you gather should contain system data about response time, processor (CPU) usage, and disk I/O and data about the query, retrieve, document routing, and folder operations.
5. Based on the two sets of data, determine whether the time-optimized ACL mode or the space-optimized ACL mode is the most beneficial for the test system.

If needed, use the procedure to change the ACL optimization mode to change the mode on your production system.

Related information

 IBM Content Manager Information Roadmap

Connecting content servers to IBM Information Integrator for Content

To enable you to connect to disparate content servers, IBM Content Manager provides a component called IBM Information Integrator for Content.

A content server is a repository for multimedia, business forms, documents, and related data, along with metadata, that allows users to process and work with the content. A business can have multiple, disparate content servers, each containing different types of information. When there is no way to effectively connect the disparate content servers, a business can waste time and money by duplicating information or training employees to perform multiple searches. Through its federated search capability, IBM Information Integrator for Content enables users to connect to and search across multiple disparate content servers.

IBM Information Integrator for Content recognizes several types of content servers, depending on the platform.

Table 5. Supported content servers by platform

Operating System	Supported server types
Windows	<ul style="list-style-type: none">• Content Manager Version 8• Content Manager for AS/400®• OnDemand for iSeries®
AIX, Linux, Solaris	<ul style="list-style-type: none">• Content Manager Version 8• OnDemand for iSeries™
z/OS	ImagePlus® for OS/390®

In addition, you can create a custom server type to define a content server of a type other than one of those provided.

You must define the content servers where information is stored before creating a search template or performing a federated search. To define a content server, you select the server type and define the details for that specific server and connection.

Before you define a server, you must know some basic information about the connectors, which are the mechanisms that enable IBM Information Integrator for Content to communicate with content servers. IBM Information Integrator for Content has a connector for each of the content servers it can connect to.

- Which connectors did the installer select? The installed connectors are listed in the `cmbcs.ini` configuration file, located in the `IBMCMROOT\cmgmt` directory.
- Did the installer select a local or remote connector option? The `cmbcs.ini` file contains the local or remote connector types.

You configure your client with local connectors if you want to connect directly to one or more content servers. A client with local connectors can improve response time, but can require more disk space and a faster processor.

You configure your client with remote connectors to eliminate the need to upgrade connectors when systems change, but can worsen response time.

IBM Information Integrator for Content supports configurations that include both local and remote connectors so you can connect directly to some local content servers and connect remotely to others.

- If your system is configured for Remote Method Invocation (RMI), is the RMI server started?

RMI allows multiple IBM Information Integrator for Content clients to search content servers through connectors installed on one RMI server. If you plan to use RMI to connect clients to content servers, you do not need the remote content server connectors on IBM Information Integrator for Content client machines. You must write all custom client applications in Java to take advantage of RMI.

To start RMI on the local RMI server, use **Start > Programs > IBM Information Integrator for Content > Start RMI Servers**. If your system uses remote RMI, look in `cmbsvclient.ini` to find the remote server where the RMI connectors are installed. Ask the RMI server administrator for more information.

- If the installer included the IBM Information Integrator for Content for iSeries connector, what information was included in the network table named `frnolint.tbl`? The `frnolint.tbl` is in *IBMCMROOT*.
- If you are defining remote content servers that contain relational databases, such as IBM Content Manager Version 8, you must catalog or add the database from the server where you are using the system administration client.

You can define a content server type that is not one of the predefined server types, but you must provide the Java or C++ connector classes and the server definition class for the new server type. You also need the Java connector to run the server inventory. For instructions about adding content servers, see the *Application Programming Guide* and the *IBM Information Integrator for Content Application Programming Reference*.

Defining servers

You must define the content server before you can connect to it and perform a server inventory.

The following list provides general steps for defining a server:

1. Right-click **Servers** in the navigation pane and click **New**. A list of the available server types displays.
2. Select a server from the list. The **New Server** window displays.
3. **Optional:** You can also create your own content server. After you create your content server, you can see the server name when you right-click the **Servers** icon.
4. Enter the server name and description in the **Server Name** field on the **General** tab. For some servers, you type only the database name. For other servers, you type in the fully qualified name of the server where the database is installed.
5. Specify initialization parameters, if required. Some servers require initialization parameters, such as connect string and configuration strings. Other servers only require the database name.
6. Click **Test Server Connection**. IBM Content Manager logs on to some content servers using the user ID and password you entered to start the system administration client. If the content server requires a different user ID and password, you are prompted to enter a valid user ID and password specific to the content server to which you are connecting.

Defining server types

You can create a custom server type, which you can use to define a content server of a different type than those provided.

Use the Server Type Definition window to create your own content server type.

After you create the content server type, right-click **Servers** and click **New** to define a content server of this type.

Restriction: You cannot modify or remove a server type definition after you save it.

To create your own content server type, complete the following steps:

1. Click **Tools** on the menu bar.
2. Select **Server Type Definition**.
3. In the **Server type name** field, enter a name for the new content server.
4. In the **Server type** field, specify a type for the new content server. This type must match the type for the associated connector.
5. In the **Java connector class** field, enter the name of the connector class to be used with the Java applications.
6. In the **C++ connector class** field, enter the name of the connector class to be used with the C++ applications.
7. In the **Server definition class** field, type the name of the server definition class to be used for creating a server of this type. Each content server uses the definition class as the primary interface to the IBM Content Manager database. For more information about the server definition class, see the *Application Programming Reference*.
8. Click **OK** to save the server type definition and close the window.

Connectors

The connectors provide the communications interface between IBM Information Integrator for Content clients, the content servers, and the system administration database.

The content server connectors, such as the IBM Content Manager Version 8 connector, provide the functionality that allows IBM Information Integrator for Content to log on to the server, search for information, and return the information to the system administration or user clients.

IBM Information Integrator for Content provides the following connectors:

- Content Manager connector for Content Manager Version 8 servers.
- Content Manager OnDemand connector for Content Manager OnDemand Version 7.1.
- Content Manager for VisualInfo for AS/400 Version 4.3 and Version 5.1.
- OS/390 connector for ImagePlus for OS/390 Folder Application Facility Version 3.1 and ImagePlus for OS/390 ODM Version 3.1.

Defining connection and configuration strings

Some content servers require initialization parameters such as connection strings and configuration strings.

The following tables show the valid connection and configuration strings for different content servers.

Important: URLs are supported for Java only. Also, when specifying multiple connection or configuration strings, separate the strings with a semicolon (;).

Table 6. Content server connection strings

Content server	Connection string	Definition
IBM Content Manager	NPWD= <i>newpassword</i>	Specifies a new password

Table 7. Content server configuration strings

Content server	Configuration string	Definition
Content Manager	CC2MIMEURL=(<i>url</i>)	Specifies the cmbcc2mime.ini file in a URL (optional). Use this string or the CC2MIMEFILE string.
Content Manager	CC2MIMEFILE=(<i>filename</i>)	Specifies the cmbcc2mime.ini file (optional). Use this string or the CC2MIMEURL string.

Defining an IBM Content Manager Version 8 server

Restriction: When you use the Linux administration client, you can only log on to Linux databases, but you can connect to a Version 8 server or a Content Manager OnDemand server on other operating systems.

Important: If the IBM Content Manager database is a DB2 database, before you can define a remote IBM Content Manager server, you must catalog the database on the server where you installed the system administration client.

To define an IBM Content Manager server, complete the following steps:

1. Enter the name of your content server. **Important:** Use the name of the database, not the host name. Use capital letters when you type the server name.
2. **Optional:** Enter a description to help you identify your content server.
3. Click the **Initialization Parameters** tab to display the Initialization Parameters page. This page shows the specific fields for an IBM Content Manager Version 8 server. When you define a Version 8 server, you are only required to type the database name. Do not change the default settings in the Initialization Parameters tab.
4. **Optional:** In the **Configuration string** field, type multiple connection string keywords and value pairs delimited by semicolons. Use the configuration string you use to connect to a DB2 server.
5. Enter the parameters necessary for connecting to the server in the **Connect string** field. Use the connect string you use to connect to a DB2 server.
6. Click **Test Connection** to test whether you can connect to this server. A message window opens to inform you of the status of the connection. If user mapping is not enabled or no mapping is available, you are prompted for a user ID and password to connect to the server. If user mapping is enabled, IBM Information Integrator for Content verifies access to the server.
7. Click **OK** to save this server definition and close the window.

Defining an ImagePlus for OS/390 server

To define an ImagePlus server, complete the following steps:

1. Enter the name of your content server. **Important:** Use the name of the database, not the host name.
2. **Optional:** Enter a description to help you identify your content server.
3. Click the **Initialization Parameters** tab to display the Initialization Parameters page. This page shows the specific fields for an ImagePlus for OS/390 server.
4. In the **FAF port number** field, enter the TCP/IP port number for the Folder Application Facility (FAF) for the ImagePlus for OS/390 server to use.
5. In the **FAF application ID** field, enter the ID for the FAF application.
6. In the **FAF protocol** field, enter the number for the FAF protocol. Use 4000 for CICS® and 4500 for IMS™.
7. In the **FAF IP address** field, enter the TCP/IP address for the FAF.
8. In the **Object distribution manager CICS** field, accept the default value 4000.
9. In the **Object distribution manager IP address** field, enter the TCP/IP address for the Object Distribution Manager.
10. In the **Object distribution manager port number** field, enter the TCP/IP port number for the Object Distribution Manager.
11. In the **Object distribution manager terminal ID** field, enter the terminal ID for the Object Distribution Manager. You can leave this field blank.
12. In the **Additional parameters** field, enter any additional parameters, such as connection strings or initialization strings, necessary for connecting to the server. You can enter multiple connection string keyword and value pairs delimited by semicolons (;).
Requirement: If you want to type the connection string keyword and value pairs, as well as the initialization string keyword and value pairs in this field, you must type the connection string keyword and value pair first, and then type two semicolons to separate the two sets of keyword and value pairs.
13. Click **Test Connection** to test whether you can connect to this server. A message window opens to inform you of the status of the connection. If user mapping is not enabled or no mapping is available, you are prompted for a user ID and password to connect to the server. If user mapping is enabled, IBM Information Integrator for Content verifies access to the server.
14. Click **OK** to save this server definition and close the window.

Tracing in IBM Content Manager ImagePlus for OS/390

Tracing can help you solve problems if you cannot connect to the Content Manager ImagePlus for OS/390 server. If you installed the connector for Content Manager ImagePlus for OS/390, you can turn on tracing for ImagePlus for OS/390 by modifying the `eyapi.ini` file that is located in `IBMCMROOT`.

The `eyapi.ini` file contains the following lines:

```
; Path where the IPFAF files are stored
; (MUST NOT have a trailing '\')
; -- default is the <ROOT Directory>\
;
IPFAFPath=d:\IBMCMROOT
; Flag for Logging (EYPLmdd.LOG files)
; -- default is Logging OFF (0)
; -- 0 All Logging OFF
```

```

; -- 1 Log files created only error conditions logged
; -- 2 Log files created all conditions logged
;
Logging = 0

;-----
;
; Flag for Logging the FAF Parameters Types created by APIs
;      -- default is Logging OFF (0)
;      -- 0 Parameter types Not logged
;      -- 1 Log Faf Parameter Types
;
FafTypeLogs = 0

```

IPFAFPath

Specifies the directory where the logs are written. The log files are named:

EYPmdd.LOG

where *mdd* is the month and day the log was created.

Logging

Specifies when a log file is created.

- 0** Do not log. The default setting is 0.
- 1** Created log files contain only error conditions.
- 2** Created log files contain all conditions.

FafTypeLogs

Specifies logging for the FAF parameter types created by APIs.

- 0** Do not log parameter types; the default setting is 0/.
- 1** Log FAF parameter types.

Defining the Content Manager OnDemand server

The Content Manager OnDemand server and library server daemon must be running before you can define a Content Manager OnDemand server. Before you define the Content Manager OnDemand server, you can ping it to verify that the server and daemon are running.

Content Manager OnDemand requires that a socket is kept alive during connection.

To define the server, complete the following steps:

1. Enter the name of your content server.

Important: Enter the partially or fully qualified host name, or the IP address of the machine on which the OnDemand server listener is running.

2. Optional: Enter a description to help you identify your content server.
3. Click the **Initialization Parameters** tab to display the Initialization Parameters page. This page shows the specific fields for a Content Manager OnDemand server.
4. Optional: Enter the port number of the Content Manager OnDemand server in the **Port number** field. If the person who installed Content Manager OnDemand selected the default port value of 0 during installation, type 0 in the port number field. If the installer selected a different port number, enter

that port number preceded by a # sign. For example, # 5000 might be an alternate port number chosen for Content Manager OnDemand on a Windows server.

5. In the **Additional parameters** field, type any additional parameters, such as connection strings or initialization strings, necessary for connecting to the server. You can type multiple connection string keyword and value pairs delimited by semicolons (;).

Requirement: If you want to type the connection string keyword and value pairs, as well as the initialization string keyword and value pairs in this field, you must type the connection string keyword and value pair first, and then type two semicolons (;;) to separate the two sets of keyword and value pairs.

If you are defining a Content Manager OnDemand server that was installed on an AS/400 server running Version 4 software, you must enter the following information in the **Additional parameters** field: STATECONNECT=#1.

If you are defining a Content Manager OnDemand server that was installed on an OS/390 server running Version 2.1 software, enter the custom port number designated when Content Manager OnDemand was installed on the OS/390 Version 2.1 server.

6. Click **Test Connection** to test whether you can connect to this server. A message window opens to inform you of the status of the connection. If user mapping is not enabled or no mapping is available, you are prompted for a user ID and password to connect to the server. If user mapping is enabled, IBM Content Manager verifies access to the server.
7. Click **OK** to save this server definition and close the window.

Working with the Content Manager OnDemand connector TCP/IP tuning and sockets

A known Windows problem might affect performance when connecting to a Content Manager OnDemand server. During repeated searches and retrievals on a Content Manager OnDemand server, many Windows sockets are opened and closed. Two default Windows settings might impact heavy traffic between IBM Content Manager and a Content Manager OnDemand server:

- When an application closes a Windows socket, Windows places the sockets port into TIME_WAIT status for 240 seconds; during this time the port cannot be reused.
- Windows limits the number of ports that an application can use to 5000.

To avoid the problems that might result, change the values for the timeout wait time and number of ports using the Windows registry editor.

- Change the value of the timeout wait time from 240 seconds to a lower number (the valid range is 30-300 seconds). The key's name is HKEY_Local_Machine\System\CurrentControlSet\services\Tcpip\Parameters\TcpTimedWaitDelay.
- Increase the maximum port number from its default of 5000 to a higher number (the valid range is 5000-65534). The key's name is HKEY_Local_Machine\System\CurrentControlSet\services\Tcpip\Parameters\MaxUserPort

For more information on TcpTimedWaitDelay and MaxUserPort, consult your Windows documentation.

Defining an IBM Content Manager for AS/400 server

To define an IBM Content Manager for AS/400 server, complete the following steps:

1. Click the **Initialization Parameters** tab to display the Initialization Parameters page. This page shows the specific fields for an AS/400 server.
2. In the **Additional parameters** field, type any additional parameters, such as connection strings or initialization strings, necessary for connecting to the server. You can type multiple connection string keyword and value pairs delimited by semicolons (;).

Requirement: If you want to type the connection string keyword and value pairs, as well as the initialization string keyword and value pairs in this field, you must type the connection string keyword and value pair first, and then type two semicolons (;;) to separate the two sets of keyword and value pairs.

Click **Test Connection** to test whether you can connect to this server. A message window opens to inform you of the status of the connection. If user mapping is not enabled or no mapping is available, you are prompted for a user ID and password to connect to the server. If user mapping is enabled, IBM Content Manager verifies access to the server.

Click **OK** to save this server definition and close the window.

Connecting to multiple Content Manager for AS/400 servers

If you use more than one AS/400 server, you must define the additional servers in the network table. The network table (*frnolint.tbl*) is located in *IBMCMROOT*. For the new server, type the server name, connection type (for example, IP network address), host name, port, and server type. For the first server, the installer types in server, host name, and port values during installation to create *frnolint.tbl*.

The following information is a typical example of information stored in *fronlnt.tbl*:

```
/* VI/400 Network Table */  
SERVER: VI400 REMOTE TCPIP  
        HOSTNAME = vi400  
        PORT     = 29000  
        SERVER_TYPE = FRNLS400
```

Viewing or modifying an existing content server definition

To maintain an efficient system, you need to view and update the content servers that IBM Information Integrator for Content uses.

The tasks that you might need to do include deleting servers that your system no longer accesses or updating the settings that the servers use. In addition, you might need to check the settings without modifying them.

To view or modify an existing content server, complete the following steps:

1. Click **Servers** to display the defined content servers in the right pane.
2. Right-click a content server and select **Properties**. The Server Properties window opens where you can view or modify any property except the name.
3. If you modify properties, click **OK** to save the server definition and close the window.

Copying a content server definition

You can copy an existing content server to define your own content server.

You can copy a content server definition when the settings of the existing content server are like the new content server that you want to define.

To copy a server definition, complete the following steps:

1. Click **Servers**. The names of the defined content servers are displayed in the right pane.
2. Right-click a defined server and select **Copy**. The Copy Server window opens.
3. Enter a name for the new server in the **Name** field.
4. Modify the properties as appropriate.
5. Click **Test Connection** to make sure you can connect your new server.
6. Click **OK** to save the new content server definition and close the window.

Defining and configuring resource managers in IBM Content Manager

Your first resource manager is deployed and configured automatically during installation. You can make changes to many of the settings. You can also add new resource managers. If you want to set up additional resource managers, you need to perform the following tasks:

1. Deploy the resource manager in WebSphere Business Integration Server Foundation or WebSphere Application Server. See *Planning and Installing Your Content Management System* for information about deploying a resource manager. Make note of the following information about the new resource manager:
 - Server name
 - Server type
 - Host name
 - User name and password
 - Protocol
 - Port
 - Schema
 - Path

Important: The user ID and password to the resource manager are stored in the resource manager definition and must match the user ID and password on the resource manager. If you change the password on the resource manager, be sure to update the resource manager definition.

2. If you are configuring a resource manager on UNIX or Windows, test the SSL connection.
3. Make sure that the resource manager is started.
4. Define the new resource manager in the library server:
 - UNIX or Windows resource manager
 - z/OS resource manager
5. Optional: If you enabled LAN cache or plan to use IBM Tivoli® Storage Manager, modify the staging area properties to meet your needs.
6. Configure the resource manager.
7. Set up server definitions among all existing resource managers.
8. Optional: Set up additional object storage options, including collections and volumes, for the resource manager. A new resource manager already has a collection and storage system, but you might want to add additional storage, such as file system volumes, Tivoli Storage Manager storage.

Related reference

“Troubleshooting the resource manager” on page 628

Resource manager

The resource manager is the repository for content stored in the IBM Content Manager system. Objects are stored in the resource manager, and the associated attribute data is stored on the library server.

When a user requests an object, the client application requests the location of the object from the library server. The library server returns the location (the resource manager that owns the object), a security token, and a timestamp indicating when the object was last updated on the resource manager. The client application then obtains the object from a resource manager using the security token. This process is illustrated in Figure 1.

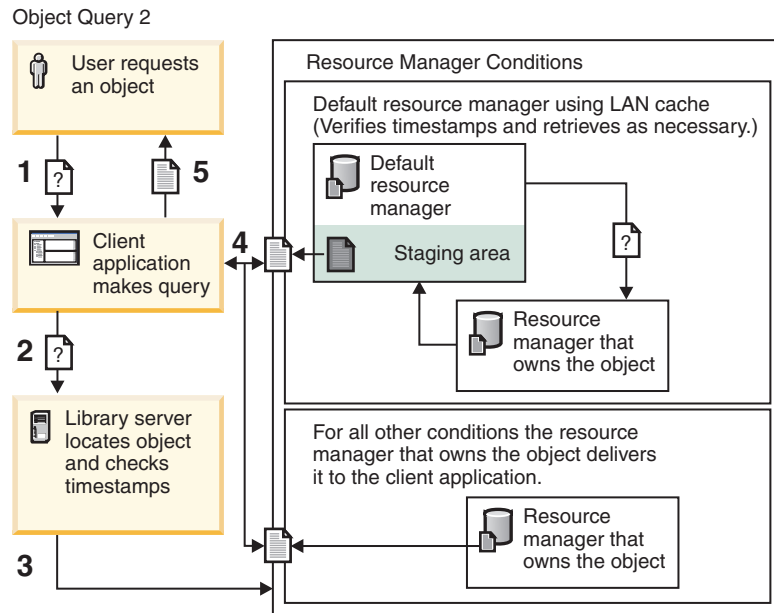


Figure 1. The path of a request from a user for an object.

Which resource manager delivers the object depends on several factors:

- Does the user ID have a default resource manager associated with it?
- If there is a default resource manager, is LAN cache enabled?
- If LAN cache is enabled, where is the object located?
- If LAN cache is enabled, does the cached copy have the same timestamp as the original?

LAN cache is not supported on resource managers on z/OS, although objects retrieved from them can be cached in the staging area of resource managers on other operating systems.

Table 8. Determination of object retrieval

Is there a default resource manager?	Is the default resource manager using LAN cache?	Where is the object located?	Do the timestamps match?	Retrieval process
No	n/a	Any resource manager	n/a	The resource manager that owns the object delivers it to the client application.

Table 8. Determination of object retrieval (continued)

Is there a default resource manager?	Is the default resource manager using LAN cache?	Where is the object located?	Do the timestamps match?	Retrieval process
Yes	No	Any resource manager	n/a	The resource manager that owns the object delivers it to the client application.
	Yes	Default resource manager	n/a	The default resource manager delivers the object to the client application.
		Other resource manager	No match or object not in staging area	The default resource manager obtains the object from the resource manager that owns the object, places a copy in its staging area, and delivers the object to the client application.
			Yes	The default resource manager delivers the object to the client application from the staging area.

Example: To illustrate how the staging area is used, suppose that you have offices in two cities, that there is a resource manager in each city, and that all user IDs have been set up with the local resource manager as the default resource manager. So users in London have the resource manager in London as their default resource manager, and users in Paris have the resource manager in Paris as their default resource manager. Further, suppose that the resource manager in London is set up to use LAN cache, but the one in Paris is not.

Assume that a user in London requests an item, and that the library server finds the object on the resource manager in London. In this case, the resource manager in London fulfils the request. The staging area is not involved, because the item was already on the resource manager.

If, however, the library server finds the object on the resource manager in Paris, the client application still asks the resource manager in London to get the object, because that is the user's default resource manager. Now, the resource manager in London checks to see if it has a copy stored locally. If the local copy has the same timestamp, then the resource manager returns it to the client application. If the timestamps do not match, the resource manager in London gets the newer copy from the resource manager in Paris, puts the newer version in its staging area, and returns the object to the client application. Any users who have the resource manager in London as their default resource manager will also retrieve the cached copy so long as its timestamp matches the library server.

Now assume that a user in Paris requests an item and that the library server returns the location as London. Because the resource manager in Paris does not use LAN cache, the client application used in Paris always gets that object from the resource manager in London.

Keep in mind that a user ID's default resource manager is the same no matter where that user logs in. So in the example, if a user whose ID was created in London with the London resource manager as the default resource manager goes to the Paris office and logs in to the IBM Content Manager system there, that user is still going to the resource manager in London for all requests.

Related reference

“Troubleshooting the resource manager” on page 628

Resource manager background services

The resource manager provides two background services: *asynchronous delete* and *asynchronous reconciliation*.

Both services cause the resource manager to synchronize with the library server and perform the following actions:

Asynchronous delete

When the background service cycle reaches this service, data that is already deleted in the library server is deleted in the resource manager. The asynchronous delete service also removes all of the data that has a OBJ_STATUS value of D in the RMOBJECTS table.

Asynchronous reconciliation

When the background service cycle reaches this service, the resource manager calls the commit or rollback methods for those transactions that are listed as expired data in the RMTRANSACTIONS table.

The default background service cycle time is 30 minutes. To change the cycle time, you can modify the BACKGROUND_SERVICE_CYCLE parameter in the RMCONFIGURATION table in the resource manager database.

When your system is not logged in to the resource manager, the resource manager background services do not run.

Resource managers on z/OS

In this section, general background information is provided about the z/OS resource manager, in addition to specific information about administering it.

Attention: You do not use the system administration client to install Object Access Method (OAM).

You must install and customize OAM before you can operate the z/OS resource manager. The resource manager uses OAM to manage storage and retrieval of objects. To use the resource manager to prefetch objects from optical storage or tape, you can define a prefetch collection name, associating with it a storage class which directs objects to hard disk drive for quicker access. The permanent object still resides in its original collection on optical or tape storage. For more information, see *IBM z/OS: Object Access Method Planning, Installation, and Storage Administration Guide for Object Support* (SC35-0426) for your level of z/OS.

Differences between the resource manager for z/OS and the resource manager for UNIX and Windows

The IBM Content Manager resource manager for z/OS differs from the resource manager for UNIX and Windows in several fundamental ways. Because of these differences, the process for defining a z/OS resource manager is different in the system administration client.

Unlike the resource manager for UNIX and Windows, which is a Java servlet running under WebSphere Business Integration Server Foundation or WebSphere Application Server, the z/OS resource manager is a fast-CGI program that runs under the IBM HTTP Server for z/OS. It is a single, dynamically loaded module. IBM Content Manager client applications communicate with the z/OS resource

manager through HTTP requests. Each HTTP request contains an "order" label, like "order=retrieve", that dictates what action is to be taken by the resource manager. On a retrieve order, for example, the resource manager extracts the object name from the incoming request, invokes the z/OS Object Access Method (OAM) to retrieve that object, and sends a reply to the client with the object.

The z/OS resource manager can perform the following functions:

- Store an object
- Retrieve an object
- Replace an object
- Query object metadata (size, creation date, SMS collection name, storage class, management class, and similar data)
- Change object SMS information (storage class, management class, retention period, collection name, and similar data)
- Prefetch an object

The IBM Content Manager resource manager stores objects in OAM. OAM divides an object into segments, and stores them as rows in DB2 tables. In addition to providing the benefits of a database manager such as DB2 Universal Database, OAM allows customers to set up predefined Data Facility Storage Management Subsystem (DFSMS) storage classes and management classes, which dictate the placement, migration, and backup of individual objects. In this way, the z/OS resource manager can use the robust data management features of DFSMS, as opposed to performing its own data management.

Alternatively, the resource manager for other operating systems stores objects as files in the file system of its operating system. The resource manager for other operating systems also performs its own migration and backup actions, requiring the system administrator to first define storage management policies through the system administration client.

System administration client functions that are not supported for z/OS resource managers

Many of the system administration client windows that are associated with UNIX and Windows resource managers are not available when you define a z/OS resource manager. These include:

- Configurations
- Device managers
- Storage classes
- Storage systems
- Storage groups
- Migration policies
- Workstation collections
- Server definitions

These either do not apply for the z/OS resource manager, or they are defined in OAM.

Prefetch

A resource manager on z/OS can be configured to move objects from one type of slow media, such as tape, to fast media, such as disk, using a prefetch process. This process allows you to make objects with predictable access needs more rapidly available to your users. For example, if you know that your users perform

annual reviews of customer records, you can set up prefetch so that the records (the objects) move from tape archives to disk just as your users need to access them.

The prefetch copy is essentially a read-only copy. If changes are made to the object, the original version is updated. No additional migration or updates are required.

Restriction: Support for prefetch is through certain Java APIs. The system administration client and client for Windows do not support prefetch.

Prefetch works by reading records in a table, ICMRMPREFETCH, for each object that will be copied. Once the records are in the table, use the ICM MOSAP asynchronous process to copy the objects to the target location.

An entry in each record indicates the status of the prefetch operation for that object. If the prefetch has not completed when a user requests the object, the object is retrieved from its original location. If an update is performed on the object prior to completion of the prefetch, the prefetch of that object is cancelled.

For more information about enabling prefetch, see the *Application Programming Guide* and *Application Programming Reference*.

Availability

The IBM Content Manager Version 8 resource manager for z/OS can run in a single z/OS image (LPAR) on a single z/OS supported mainframe or across several z/OS supported mainframes using parallel sysplex technology. Parallel sysplex provides a way to present up to 32 z/OS supported mainframes. Sysplex Distributor (SD) provides a single image view of z/OS systems to a user. When using SD, the SD TCP/IP address must be defined to the IBM Content Manager z/OS library server for the resource manager and not the actual HTTP address where the resource manager is running.

The HTTP Server can use the capabilities of the Sysplex Distributor. It allows you to define policies for routing incoming requests to backup z/OS resource managers if the primary LPAR or processor of the HTTP Server is unavailable. Should the HTTP Server become unavailable, the Sysplex Distributor routes both existing and new connections to the backup server or servers. It automatically determines what the service goals are (using data from Workload Manager) and where the work can be accomplished most efficiently. The Sysplex Distributor then routes the work accordingly. In this way, it ensures that the HTTP Server is always available. The switch to backup servers is transparent to clients.

For details on how to define your HTTP Server to the Workload Manager, see IBM z/OS: *HTTP Server Planning, Installing, and Using* (SC34-4826).

Scalability

The Workload Manager, with the Sysplex Distributor, helps to ensure that the z/OS resource manager performs well, that it scales to accommodate IBM Content Manager workloads, and that it is reliable. The HTTP Server under which it runs should be defined to the Workload Manager on your z/OS system. Assign it a service policy that prioritizes the incoming IBM Content Manager requests appropriately with other work on that system.

You can set up the z/OS HTTP Server to take advantage of the features of the z/OS Workload Manager that:

- Reroutes the HTTP request to the place in the sysplex which can accommodate it if the resource manager primary instance is failing.
- Takes back the work from the backup instance of the resource manager once the primary resource manager is restored to working order.

The z/OS resource manager runs under the HTTP Server z/OS, which is a multi-threaded process handling multiple incoming HTTP requests at a time. You can define the HTTP server to Workload Manager and associate it with a service class. The service class tells Workload Manager what the performance goals are for its work. Workload Manager then prioritizes the HTTP server workload according to those goals as it searches the sysplex (or parallel sysplex) for resources. As HTTP requests come in, Workload Manager might create several address spaces within the sysplex to complete them in the most efficient way possible, starting and stopping address spaces as necessary.

For example, Workload Manager might start an address space with a maximum number of 50 active threads. If an HTTP request comes in, and all 50 worker threads are busy, Workload Manager starts a new address space to handle it. Workload Manager also maintains this second address space as long as necessary. After Workload Manager determines that the new address space is no longer needed, Workload Manager automatically stops it. Externally, this resource manager is still defined to IBM Content Manager as a single instance of the HTTP Server listening at a single port. It is all transparent to IBM Content Manager clients.

Testing the SSL connection

The resource manager requires Secure Sockets Layer (SSL) to allow administration by the system administration client. You also need to enable both HTTP and HTTPS access for the resource manager to be fully functional. All of this might already be configured. Use the following procedure to see if SSL is already enabled.

Attention: During installation, either IBM HTTP Server or WebSphere Application Server was selected to manage SSL connections. The URLs that you enter to test the SSL connection depend on which method is used. For all URLs, make the following substitutions:

host Fully qualified hostname of the resource manager.

Important: When working with SSL, never specify localhost as the hostname. SSL requires that you use a valid workstation hostname.

port Listening port defined for HTTP or HTTPS connections.

Tip: The port number is typically 9081 for HTTP connections and 9444 for HTTPS connections. If those values do not work, check the HTTP transport settings in WebSphere Application Server.

resource_manager

Resource manager application server name. The default resource manager name is icmrm.

1. If it is not already running, start the resource manager.
2. Open a Web browser.
3. Test the HTTP connection. Enter the appropriate URL in the browser.

SSL manager	URL	Expected result
IBM HTTP Server	<code>http://host</code>	Welcome page
WebSphere Application Server	<code>http://host:port</code>	Virtual host or web application not found page

4. Test the HTTPS (SSL) connection. Enter the appropriate URL in the browser.

SSL manager	URL	Expected result
IBM HTTP Server	<code>https://host</code>	Welcome page
WebSphere Application Server	<code>https://host:port</code>	Virtual host or web application not found page

5. View the **snoop** information provided by the resource manager for a regular connection. Enter the appropriate URL in the browser.

SSL manager	URL	Expected result
IBM HTTP Server	<code>http://host/resource_manager/snoop</code>	snoop results
WebSphere Application Server	<code>http://host:port/resource_manager/snoop</code>	snoop results

6. View the **snoop** information provided by the resource manager for a secure connection. Enter the appropriate URL in the browser.

SSL manager	URL	Expected result
IBM HTTP Server	<code>https://host/resource_manager/snoop</code>	snoop results
WebSphere Application Server	<code>https://host:port/resource_manager/snoop</code>	snoop results

If the test is successful, SSL is already configured and you don't need to make any changes. If the test fails, you need to configure SSL or modify the existing configuration. SSL configuration is discussed in the IBM HTTP Server Information Center.

Related information

 WebSphere Application Server, Version 6.1

Defining a resource manager

The resource manager is the component of an IBM Content Manager system that manages objects. Users store and retrieve digital objects on the resource manager by routing requests through the library server. Before that, you must assign a resource manager to a library server in the system administration client.

Restriction: To define a resource manager, you must have one of these system defined privileges:

- ICM_PRIV_DOMAIN_DEFINE_RM
- ICM_PRIV_DOMAIN_ADMIN
- ICM_PRIV_SUPER_DOMAIN_ADMIN

By default, the user account icmadmin has the required privileges to define a resource manager.

After deploying a new resource manager, you must create a definition for it in IBM Content Manager.

To define a resource manager:

1. Expand your library server in the tree view.
2. Right-click **Resource Managers** and click **New**. The New Resource Manager Definition window opens.
3. In the **Name** field, type the name of the resource manager that you want to define.

Restrictions:

- The name must be unique. Although the system administration client will allow you to create resource managers that are unique only by case, problems might arise if you do so because DB2 Universal Database is case insensitive. For example, the system administration client considers Resource and RESOURCE to be unique names, but the DB2 database considers them to be the same.
 - The name must exactly match the name of the resource manager database. This restriction is true for both local and remote resource managers.
 - The name cannot include a colon (:) character.
4. If you have enabled administrative domains, select a domain from the list in the **Admin Domain** field.
 5. In the **Hostname** field, enter the fully qualified host name or IP address of the resource manager.
 6. From the **Application server operating system** list, select the operating system of the resource manager application. This field relates to the operating system of the application server, not to the operating system of the resource manager database that might reside on a different machine.
 7. In the **User ID** field, enter the user ID used to log on to the resource manager.
 8. In the **Password** field, enter the password for the user ID.
 9. Optional: Select the **Enable LAN cache** check box to move objects from a remote resource manager to the local or default resource manager. Enabling the LAN cache can increase network efficiency when the remote resource manager is distant from the library server or when you frequently access specific objects.
 10. Optional: You can indicate that a server is not available, for example, because it is being repaired. Select the **Server is unavailable** check box to prevent clients from attempting to retrieve objects from this server. The clients attempt to retrieve objects from other resource managers.
 11. In the **Token duration** field, type the number of seconds after which the token provided to the client for object access expires. A token is used for security purposes to allow users access to objects. The token duration indicates how long an object sent from the library server to the resource manager remains valid. The default duration is 2 days. The token duration is set for the resource manager, and cannot be set at the object level.

Tip: Set the token duration according to your particular needs, considering your applications and the latency between the library server and the resource manager. Decreasing the duration is a security improvement, but there are

situations where a longer duration is required. For example, five minutes is a reasonable duration for many applications, but you might want to set it to 30 minutes to match the default timeout for WebSphere Business Integration Server Foundation and WebSphere Application Server applications. Your particular needs might even require a longer duration. For example, if the URL to retrieve an object must be sent by e-mail, a duration of 30 minutes is probably not long enough.

Important: Make sure that the clocks on the library server and resource manager are synchronized. If the systems are not in the same time zone, use Greenwich Mean Time (GMT) for the server clocks.

12. Add access information for the resource manager. Click **Add** to open the New Access Type window. If you need to modify or delete an access type, click **Modify** or **Remove**, respectively.
13. Click **OK** to save the information and close the window.

Related concepts

“Managing object storage in IBM Content Manager” on page 319

Defining a resource manager on z/OS

You define your default resource manager during installation. You can also define additional resource managers using the system administration client.

Tip: You must know the following information to define a z/OS resource manager. The other fields are not used by z/OS resource managers.

- Server name
- Host name
- Platform
- Protocol
- Port number
- Access type data
- If applicable, a valid RACF® user ID and password for that z/OS system

To define a resource manager that is located on z/OS:

1. Expand your library server in the tree view.
2. Right-click **Resource Managers** and click **New**. The New Resource Manager Definition window opens.
3. In the **Name** field, type the name of the resource manager that you want to define.

Restrictions:

- The name must be unique. Although the system administration client will allow you to create resource managers that are unique only by case, problems might arise if you do so. For example, the system administration client considers Resource and RESOURCE to be unique names. The supporting database, DB2 Universal Database, is case insensitive, and considers the two names to be the same.
 - The name cannot include a colon (:) character.
4. If you have enabled administrative domains, select a domain from the list in the **Admin Domain** field.

5. In the **Hostname** field, enter the fully qualified host name or IP address of the resource manager.
6. From the **Application server operating system** list, select the operating system of the resource manager application. This field relates to the operating system of the application server, not to the operating system of the resource manager database that might reside on a different machine.
7. In the **User ID** field, enter the user ID used for authentication with the resource manager.
8. In the **Password** field, enter the password for the user ID.
9. Optional: You can indicate that a server is not available, for example, because it is being repaired. Select the **Server is unavailable** check box to prevent clients from attempting to retrieve objects from this server. The clients attempt to retrieve objects from other resource managers.
10. Specify the token duration in seconds. The token duration is the length of time that an object's security token that is passed to the resource manager on all requests is valid, before it expires.
11. Add access information for the resource manager. Click **Add** to open the New Access Type window. If you need to modify or delete an access type, click **Modify** or **Remove**, respectively. When specifying access type data, only HTTP applies for the z/OS resource manager. Specify the protocol, with the port number where the HTTP Server listens, and the path name /ICMResourceManager in the **Access data** field.
12. Click **OK** to save the information and close the window.

LAN cache

LAN cache allows caching of resources in the default resource manager for objects stored on other resource managers. For example, if there are several available resource managers and the client application requests an object from the default resource manager, then the client application searches other resource managers if it cannot find the object from the default resource manager. After the object is found, the object can be cached in the memory of the default resource manager, which saves time when the object is requested again.

The IBM Content Manager system administration client has a feature that allows users to enable LAN cache. If you have users who frequently retrieve the same object, enabling LAN cache can improve user efficiency by reducing the time required to retrieve and display an object stored on a remote content server.

Restrictions: LAN cache requires IBM Content Manager Version 8.2 or later on both the system administration client and the resource manager. Furthermore, both components must be using the same version and release level. A resource manager on UNIX or Windows can cache objects retrieved from a resource manager on z/OS, but a z/OS resource manager cannot use LAN cache itself.

You can enable LAN cache from the New Resource Manager Definition window in the system administration client. When you enable LAN cache, the IBM Content Manager system retrieves requested objects from the remote server and stores the objects in the staging directory of the server that supports the local resource manager. When client users request the object, the system retrieves the local copy, if there is one, instead of accessing the original object on the remote server.

Each time a client attempts to retrieve the cached object, the resource manager compares the timestamp applied when the object was originally retrieved to the

timestamp of the object on the remote server. If the timestamps are different, the resource manager retrieves the updated object and overwrites the original cached object.

For example, suppose that your system has three client users who are working on an insurance claim. Each user needs to view the same large photograph of a damaged car. The photograph, which is in the .TIFF file format, is stored on a content server in a different state.

If LAN cache is not enabled, each client user requests and receives the file from the remote server. Depending on file size and network traffic, the retrieval and display process can be slow and could reduce efficiency of the client users. With LAN cache enabled, a copy is stored locally after the first request for the object. Subsequent requests receive the copy, so long as the timestamp matches.

Viewing or modifying resource manager properties

Fields that you cannot change are disabled, but the values are provided for your information.

To view or modify a resource manager's properties:

1. Expand **Resource Managers** in the tree view.
2. Right-click the resource manager and click **Properties** to open the Resource Manager Properties window.
3. If you have enabled administrative domains, in the **Admin Domain** field, select a domain from the list.
4. In the **Hostname** field, enter the host name or IP address of the resource manager.
5. From the **Application server operating system** list, select the operating system of the resource manager application. This field relates to the operating system of the application server, not to the operating system of the resource manager database that might reside on a different machine.
6. In the **User ID** field, enter the user ID used to log on to the resource manager.
7. In the **Password** field, enter the password for the user ID.
8. Select the **Enable LAN cache** check box to enable LAN cache for the server. LAN cache moves objects from a remote resource manager to the local or default resource manager. Enabling LAN cache can increase network efficiency when the remote resource manager is distant from the library server or when you frequently access specific objects.
9. Select the **Server is unavailable** check box so that a client bypasses this server when retrieving objects. The client attempts to retrieve objects from other resource managers.
10. In the **Token duration** field, type the number of seconds after which the token provided to the client for object access expires. A token is used for security purposes to allow users access to objects. The token duration indicates how long an object sent from the library server to the resource manager remains valid. The default duration is 2 days. The token duration is set for the resource manager, and cannot be set at the object level.

Tip: Set the token duration according to your particular needs, considering your applications and the latency between the library server and the resource manager. Decreasing the duration is a security improvement, but there are situations where a longer duration is required. For example, five minutes is a

reasonable duration for many applications, but you might want to set it to 30 minutes to match the default timeout for WebSphere Business Integration Server Foundation and WebSphere Application Server applications. Your particular needs might even require a longer duration. For example, if the URL to retrieve an object must be sent by e-mail, a duration of 30 minutes is probably not long enough.

Important: Make sure that the clocks on the library server and resource manager are synchronized. If the systems are not in the same time zone, use Greenwich Mean Time (GMT) for the server clocks.

11. If you want to change your resource manager access information, click **Modify**. To delete an access type, select the access type and click **Remove**.
12. Click **OK** to save the information and close the window.

Adding an access type

You add access types from the New Resource Manager Definition window or the Resource Manager Properties window.

To add an access type:

1. Click **Add** to open the New Access Type window.
2. In the **Protocol** field, select the communication protocol used by the resource manager from the list.
3. In the **Port number** field, enter the port number to which this protocol listens.
4. In the **Access data** field, type the program needed to access data. You must specify `/context_root/ICMResourceManager` where *context_root* is the resource manager Web application installation path.
5. Click **OK** to save the information.

Access type

An access type is a configuration for a communication protocol used by a resource manager. The configuration consists of the protocol type, the port number to use, and the path to the program needed to access data.

The resource manager requires one access type for HTTP and one for HTTPS.

Tip: Client APIs generally do not use HTTPS.

The usual port numbers are 80 for HTTP and 443 for HTTPS, but your system could be configured differently. If you change the port number after deploying your resource managers, you will need to update:

- The access type
- The `httpd.conf` file
- WebSphere Business Integration Server Foundation or WebSphere Application Server

See the related information about changing port numbers for instructions.

Viewing or modifying an access type

You view access types from the New Resource Manager Definition window or the Resource Manager Properties window.

To view or modify an access type:

1. Select one of the access type entries already defined for the resource manager.
2. Click **Modify** to open the Access Type Properties window.
3. In the **Protocol** field, select the communication protocol used by the resource manager from the list.
4. In the **Port number** field, enter the port number to which this protocol listens.

Important: If you change the port number, you will need to update some other settings as well. See the troubleshooting information about changing the resource manager port number.

5. In the **Access data** field, type the program needed to access data.
6. Click **OK** to save the information.

Related reference

“Changing the resource manager port number on UNIX and Windows” on page 637

“Changing the resource manager port number on z/OS” on page 638

Viewing or modifying the staging area properties

The staging area is created when you install IBM Content Manager. However, you can modify these properties to customize the staging area for your content management system.

The system administration client allows you to configure the staging area for size and purge rate. You can only have one staging area for each resource manager. To view or modify the staging area properties:

1. Expand **Resource Managers** in the tree view.
2. Right-click the resource manager that you want to work with and click **Staging Area** to open the Staging Area Properties window.
3. In the **Path** field, type 1 - 1023 alphanumeric characters as the directory path of the staging area for the resource manager. If the directory does not exist, it will be created. The staging area should be a directory that is dedicated to that purpose. The application server user ID must have write access to the directory.

Attention: Changing the path of an existing staging area does not move or delete any staged objects. You can let the server repopulate the new cache area, or you can copy the contents of the original path to the new path.

4. The **Size** box displays size limits for the resource manager staging area. In the **Set maximum size** field, type 1 - 2,147,483,647 as the number of megabytes allocated for the staging area.

Attention: The **Current size** and **Percent in use** fields show the actual usage statistics for the staging area. You cannot change these values.

5. In the **Maximum subdirectories** field, type or select the maximum number of subdirectories allocated for the staging area. The system defines the subdirectory names. Create subdirectories to manage cached objects more efficiently.
6. In the **Maximum cached file size** field, type 1 - 2,047 as the maximum cached file size in megabytes. If you set this value to 1,000 megabytes, for example, then no file with a size larger than 1,000 megabytes is cached in the staging area. If you decrease this size later, the new setting applies from that point onward. However, you do not lose previously cached objects stored under the previous setting.

Requirement: The maximum cached file size must be smaller than the maximum size for the staging area.

7. In the **Start purge when size equals % of maximum** field, type or select a value from 1 - 100 as the percentage at which the purger starts. The purger removes objects. For example, if the value in the **Set maximum size** field is 1,000 megabytes, and the purge value is set to 50%, then purging begins at 500 megabytes.
8. In the **Stop purge when size equals % of maximum** field, type or select a value from 1 - 100 as the percentage at which the purger stops.

Requirement: The stop purger percentage must be smaller than the start purger percentage.

9. Click **OK** to save the information and close the window. Click **Apply** to save the information without closing the window.

Related concepts

"Staging area"

Related tasks

"Setting the resource manager definition" on page 56

Staging area

The staging area stores cached versions of items previously requested from other resource managers and from Tivoli Storage Manager. Staging areas need fast disk drives for high-demand objects, large objects, and objects that require high-speed performance to access, like audio and video objects. Staging areas provide fast performance and allow you to access large objects that could be stored on slower devices.

When an application requests an object that is stored in Tivoli Storage Manager, the resource manager that owns the object will cache the Tivoli Storage Manager object in the staging area and return the object to the client application.

The system administration client allows you to manage the staging directory to get the most benefits from LAN caching. Staging directory management tasks include:

- Setting automatic cache purge specifications: A purge removes the oldest and least frequently used objects from the staging directory. An object that is frequently used might remain on the staging area even though newer objects that are not frequently used are purged. To configure automatic purge specifications, modify the cycles in the resource manager configuration.
- Defining subdirectories to hold cached objects: Storing cached objects in subdirectories can improve system retrieval time because the system can target the search without looking through individual objects stored in the staging directory.
- Defining the size of the staging directory: Depending on the size and volume of cached objects, you might need to modify the original parameters defined for the staging directory.
- Defining the maximum size of the cached object: The system does not cache objects that exceed the maximum size. However, if you decrease the maximum size and objects that were stored earlier exceed the new maximum size, the system retains the objects.

Creating resource manager configurations

A resource manager configuration contains the parameters that are used to define the environment for the resource manager.

To create a resource manager configuration:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Right-click **Configurations** and click **New**. The New Resource Manager Configuration window opens.
4. Click on the tab or tabs containing the settings you want to view or modify. See the related information for instructions about each tab.
 - **Definition**: Define the resource manager configuration.
 - **Services**: Define the resource manager services.
 - **Cycles**: Configure cycles and batches.
 - **Migrator Schedule**: Specify how often the migrator will run.
 - **Replicator Schedule**: Specify how often the replicator will run.
5. Click **OK** to save the information and close the window. Click **Apply** to save the information without closing the window.

Setting the resource manager definition

On the Definition page in the resource manager configuration:

1. In the **Name** field, type 1 to 16 alphanumeric characters as a name for the resource manager configuration.
2. In the **Description** field, type 1 to 80 alphanumeric characters as a description of the resource manager configuration.
3. Select the **Active** check box to activate this configuration. You can have multiple configurations for one resource manager, but only one configuration can be active at a time. If you have more than one configuration for a resource manager, selecting this box clears the selection of the other configurations.
4. Select the **Advertise accept ranges** check box to enable the ability of the resource manager server to advertise byte serving capability to the clients. Beginning with Version 8.4.3, the default behavior is to not advertise this capability. The advertisement of byte serving of documents is required only in limited circumstances, when both of the following conditions are true: when your organization must serve extremely large documents (hundreds of megabytes) over an unstable Internet connection and if your organization must create PDF documents with Adobe Fast Web View function enabled.
5. In the **Library response** field, type the required maximum amount of time in seconds that the resource manager should wait for a response from the library server. If the library server does not respond in that time period, the user receives an error message.
6. In the **Client response** field, type the required maximum amount of time in seconds that the resource manager should wait for a response from the client application. If the client does not respond in that time period, the user receives an error message.
7. In the **Purger** field, type the maximum amount of time in seconds that the resource manager should wait for a response from the purger. The purger is a function of the resource manager that removes objects from the system.

8. Click **OK** to save changes and exit or **Apply** to save changes and continue working.

Setting the cycles

On the Cycles page in the resource manager configuration:

1. In the **Purger** field, type or select the amount of time in hours and minutes that must elapse before the purger begins purging if necessary.
2. In the **Migrator** field, type or select the amount of time in hours and minutes that must elapse before the migrator checks if there is anything to migrate. This value works together with the migrator schedule settings to control how often migration takes place. Migration should be configured to take place at off-peak times. If that is not possible, set this value low to balance the load on the system.

Example: For example, you could set the **Migrator** field to 5 minutes and set the migrator schedule to run daily starting at 8:00 PM and to run for 8 hours. Then the migrator will check for objects to migrate every 5 minutes between 8:00 PM and 4:00 AM. At 3:55 AM, it will make its final check for this cycle and will complete all tasks, even if doing so lasts beyond 4:00 AM. It will then stop until its next cycle begins, that evening at 8:00 PM.

3. In the **Threshold** field, type or select the amount of time in hours and minutes that must elapse before the system checks the capacity of the volumes, if there is anything to migrate.
4. In the **Stager** field, type or select the amount of time in hours and minutes that must elapse before the stager checks if the threshold of DB2 Content Manager VideoCharger has been reached.
5. In the **Replicator** field, type or select the amount of time in hours and minutes that must elapse before the system checks to see whether replication is necessary. In the same way that the **Migrator** value controls migration, this value works together with the replicator schedule settings to control how often replication takes place. Unlike migration, however, replication should be configured to run constantly.
6. Under **Batches**, use the controls to define or change the number of files in a batch when you move objects from the staging area to volumes and from one storage class to another.
 - a. In the **Purger** field, type an integer from 1 to 9999 as the number of files in the batch during the purging process. The recommended value for this field is 1000.
 - b. In the **Migrator** field, type an integer from 1 to 9999 as the number of files in the batch when a group of files is moved from one storage class to another. The recommended value for this field is 1000.
 - c. In the **Stager** field, type an integer from 1 to 9999 as the number of files in the batch when a group of files is moved from the staging area to a volume. The recommended value for this field is 1000.
7. Click **OK** to save changes and exit or **Apply** to save changes and continue working.

Related tasks

“Creating a storage class” on page 323

Setting the services

You can use the system administration client to stop and start the resource manager services.

Table 9. Usage guidelines for resource manager services

Service	Use
Purger	If LAN cache is enabled or if Tivoli Storage Manager is in use
Migrator	Always
Stager	If DB2 Content Manager VideoCharger or another media archiver is in use
Replicator	If replicas are defined for at least one resource manager

On the Services page in the resource manager configuration:

1. Click **Refresh Now** to verify your selections.
2. Click **Cancel** if you don't want to save your changes.
3. Click **OK** to save changes and exit or **Apply** to save changes and continue working.

Setting the migrator schedule

The migrator schedule runs the migrator. The migration policy tells the system how long objects must remain in a storage class, and the migrator moves the objects between storage classes when they are scheduled to move.

Recommendation: You should run the migrator during off-peak hours, but it should run frequently.

Requirement: The migrator is a stand-alone service and it must be started for migration to occur.

On the Migrator Schedule page in the resource manager configuration:

1. Specify when you want the migrator to run:
 - Click the **Every day** radio button to run the migrator daily. You must specify a start time and duration for the migrator.
 - Click the **Specific day** radio button to run the migrator on specific days. You must specify a start time and a duration for each day that you want the migrator to run.
2. In the **Start time** field, type a value from 00:00 to 23:59 (where 00:00 is midnight and 23:59 is 11:59 p.m.) for the time that you want to begin migration.
3. In the **Duration** fields, type or select from 0 to 24 hours and from 0 to 59 minutes for how long the system should run the migrator.

Important: The default value for duration is 24 hours 0 minutes. If you do not change this value, the migrator starts at midnight and runs 24 hours.

4. Click **OK** to save changes and exit or **Apply** to save changes and continue working.

Tip: The migrator can run through overlapping schedules.

Example: For Sunday, you type 17:00 in the **Start time** field and 18 hours in the **Duration** field. For Monday, you type 8:00 for the start time. On Sunday, the system starts the migrator at 5 p.m. and runs the migrator 18 hours until Monday at 11 a.m. The system ignores the start time on Monday at 8 a.m. because the migrator is already running.

Related tasks

“Creating a migration policy” on page 352

“Creating a device manager” on page 325

Setting the replicator schedule

The replicator schedule runs the replicator. The purpose of replication is to replicate object data from a primary resource manager to a copy resource manager for enhanced retrievability and security.

Requirement: The replicator is a stand-alone service and it must be started for replication to occur.

On the Replicator Schedule page in the resource manager configuration:

1. Specify when you want the replicator to run:
 - Click the **Every day** radio button to run the replicator daily. You must specify a start time and duration for the replicator.
 - Click the **Specific day** radio button to run the replicator on specific days. You must specify a start time and a duration for each day that you want the replicator to run.
2. In the **Start time** field, type a value from 00:00 to 23:59 (where 00:00 is midnight and 23:59 is 11:59 p.m.) for the time that you want to begin replicator.
3. In the **Duration** fields, type or select from 0 to 24 hours and from 0 to 59 minutes for how long the system should run the replicator.

Important: The default value for duration is 24 hours 0 minutes. If you do not change this value, the replicator starts at midnight and runs 24 hours.

4. Click **OK** to save changes and exit or **Apply** to save changes and continue working.

Tip: The replicator can run through overlapping schedules.

Example: For Sunday, you type 17:00 in the **Start time** field and 18 hours in the **Duration** field. For Monday, you type 8:00 for the start time. On Sunday, the system starts the replicator at 5 p.m. and runs the replicator 18 hours until Monday at 11 a.m. The system ignores the start time on Monday at 8 a.m. because the replicator is already running.

Related concepts

“Replication” on page 364

Related tasks

“Creating a storage class” on page 323

“Creating a device manager” on page 325

Resource manager configuration

When you add a resource manager to your library server, you must also configure it. When you configure the resource manager, you define the rules under which it operates. You define the following settings:

- Database connections
- Timeouts
- Cycles of resource manager-related processes such as purger, migrator, and asynchronous recovery
- Schedule information for migration

Configuration takes some planning. You must analyze what types of items the resource manager manages and the pattern in which users access these items. Based on your analysis, you can decide when to purge or migrate items. You can set schedules one way now, but as your needs change, you might decide to change your schedules and cycles.

You can use the default resource manager configuration, IBMCONFIG, with or without modifications. You can also create your own custom configurations.

Related concepts

“Managing databases” on page 394

Viewing or modifying a resource manager configuration

To view or modify a resource manager configuration:

1. Expand **Resource Managers** in the system administration tree.
2. Expand the resource manager that you want to work with.
3. Click **Configurations** to display all of the resource manager configurations in the right pane.
4. Right-click the configuration you want to change and click **Properties**. The Properties window opens.
5. Click on the tab or tabs containing the settings you want to view or modify. See the related information for instructions about each tab.
 - Definition: Define the resource manager configuration.
 - Services: Define the resource manager services.
 - Cycles: Configure cycles and batches.
 - Migrator Schedule: Specify how often the migrator will run.
 - Replicator Schedule: Specify how often the replicator will run.
6. Click **OK** to save the information and close the window.

Copying a resource manager configuration

To copy a resource manager configuration:

1. Expand **Resource Managers** in the tree view.

2. Expand the resource manager that you want to work with.
3. Click **Configurations** to display all of the resource manager configurations in the right pane.
4. Right-click the configuration you want to copy and click **Copy**. The Copy window opens.
5. Click on the tab or tabs containing the settings you want to view or modify. See the related information for instructions about each tab.
 - **Definition:** Define the resource manager configuration.
 - **Services:** Define the resource manager services.
 - **Cycles:** Configure cycles and batches.
 - **Migrator Schedule:** Specify how often the migrator will run.
 - **Replicator Schedule:** Specify how often the replicator will run.
6. Click **OK** to save the information and close the window.

Deleting a resource manager configuration

Important: You cannot delete the active resource manager configuration. Either make another configuration active or stop the resource manager before deleting the configuration, then create a new configuration before restarting the resource manager.

To delete a resource manager configuration:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Configurations** to display all of the resource manager configurations in the right pane.
4. Right-click the configuration that you want to delete and click **Delete**.
5. Click **OK** to confirm the deletion.

Related concepts

"Starting and stopping a resource manager" on page 371

Adding a server definition

Every resource manager must have a server definition, which you complete by using the system administration client.

To add a server definition:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Right-click **Server Definitions** and click **New** to open the New Server Definition window.
4. In the **Name** field, enter the name of the server that is being defined.
5. Select the type of server being defined from the **Server type** list.
6. In the **Hostname** field, enter the fully qualified host name or IP address of the server.
7. In the **Platform** field, select the platform on which the server you are adding runs.
8. In the **User ID** field, enter the user ID to access the server. For a Tivoli Storage Manager server, enter the node name.

9. In the **Password** field, enter a password for the user ID.
10. From the **Protocol list**, select the communication protocol to use when communicating with this server.
11. In the **Port Number** field, enter the port number to reach the server.
12. In the **Schema** field, enter the schema to reach the server.
13. In the **Path** field, enter the path to reach the server. For a Tivoli Storage Manager server, enter the fully qualified path to the dsm.opt file.
14. In the **Client options file** field, enter the fully qualified path for the Tivoli Storage Manager client options file. For more information about this value see your Tivoli Storage Manager documentation.
15. In the **Buffer size** field, enter a value that will be used to set the buffer size to use for data transfer with a Tivoli Storage Manager server. For more information about this value see your Tivoli Storage Manager documentation.
16. In the **File space name**, enter the file space name that is used by Tivoli Storage Manager to determine where the content is located. For more information about this value see your Tivoli Storage Manager documentation.
17. In the **File space information** field, enter an identifier for resource manager objects within the Tivoli Storage Manager file space. This field is optional. For more information about this value see your Tivoli Storage Manager documentation.
18. If you want to enable the resource manager to manage and hold a passphrase that is used for encrypting content stored by the resource manager on a Tivoli Storage Manager server, select the **Enable Tivoli Storage Manager encryption** check box. When you select this check box, you must enter and confirm the passphrase in the Set Encryption Passphrase window. The passphrase must meet the Tivoli Storage Manager requirements for passphrases, with a minimum size of 6 bytes and a maximum size of 64 bytes.

Restriction: After a server definition is saved with the encryption feature enabled, you cannot change the passphrase or disable the Tivoli Storage Manager encryption feature from the system administration client.

19. Click **OK** to save the server information.

Related tasks

Configuring Tivoli Storage Manager for content encryption

Server definition

Server definitions allow resource managers to communicate with each other and with storage systems. For example, you might have a resource manager, a DB2 Content Manager VideoCharger server, and a Tivoli Storage Manager server.

A resource manager must have a server definition for all other resource managers and for every storage system it uses.

Example: For example, assume that you have two resource managers, for offices in London and Paris, and want to add one for a new office in Tokyo. After deploying the Tokyo resource manager, you must create server definitions for the London and Paris resource managers in the Tokyo resource manager configuration. You must also add a server definition for the Tokyo resource manager to both the London and Paris resource managers.

Viewing or modifying a server definition

To view or modify a server definition:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Server Definitions** to display the servers in the right pane.
4. Right-click the server that you want to view or modify and click **Properties**.
5. Select the type of server being viewed or modified from the **Server type** list.
6. In the **Hostname** field, enter the host name or IP address of the server.
7. In the **Platform** field, select the operating system on which the server that you are modifying runs.
8. In the **User ID** field, enter the user ID to access the server.
9. In the **Password** field, enter a password for the user ID.
10. From the **Protocol list**, select the communication protocol to use when communicating with this server.
11. In the **Port Number** field, enter the port number to reach the server.
12. In the **Schema** field, enter the schema to reach the server.
13. In the **Path** field, enter the path to reach the server.
14. Click **OK** to save the server information.

Copying a server definition

To copy a server definition:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Server Definitions** to display the servers in the right pane.
4. Right-click the server that you want to copy and click **Copy**.
5. In the **Name** field, enter the new name of the server.
6. Select the type of server being defined from the **Server type** list.
7. In the **Hostname** field, enter the host name or IP address of the server.
8. In the **Platform** field, select the operating system on which the server that you are adding runs.
9. In the **User ID** field, enter the user ID to access the server.
10. In the **Password** field, enter a password for the user ID.
11. From the **Protocol list**, select the communication protocol to use when communicating with this server.
12. In the **Port Number** field, enter the port number to reach the server.
13. In the **Schema** field, enter the schema to reach the server.
14. In the **Path** field, enter the path to reach the server.
15. Click **OK** to save the server information.

Deleting a server definition

To delete a server definition:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Server Definitions** to display the servers in the right pane.

4. Right-click the server that you want to delete and click **Delete**.
5. Click **OK** to confirm the deletion.

Content encryption with Tivoli Storage Manager

The resource manager server definition can include a passphrase that is used for encrypting content stored on a Tivoli Storage Manager server.

If you configure the Tivoli Storage Manager TSM client options files to encrypt content with the password prompt method, you can also configure the resource manager to provide the required passphrase for Tivoli Storage Manager to encrypt this content as it is stored to the server. To do so, you create a passphrase in the resource manager server definition. The passphrase is used to encrypt content stored by that resource manager on the Tivoli Storage Manager server.

After you create a resource manager definition that use the content encryption feature, you cannot disable this feature or change the passphrase from the system administration client.

The passphrase for Tivoli Storage Manager content encryption is stored as encrypted data in the ACC_PUBLIC_KEY column of the RMACCESS table. The RMACCESS table contains a row for each RMSEVER entry, including the Tivoli Storage Manager server.

When Tivoli Storage Manager requests the passphrase, it is passed to the Tivoli Storage Manager server in plain text and is then transformed into the key that can access the encrypted data. The resource manager uses an internal key from the ENCRYPTIONKEY_STR property of the RMCONFIGURATION table to decrypt the passphrase.

Attention: Do not alter the database properties that hold the encrypted passphrase for Tivoli Storage Manager or the resource manager encryption key. If any change is made to the value of the ENCRYPTIONKEY_STR property in the RMCONFIGURATION table, then the resource manager cannot decrypt the passwords stored in the RMACCESS table. Therefore, the passphrase for Tivoli Storage Manager server will become unusable. If any change is made to the value of the ACC_PUBLIC_KEY column for the Tivoli Storage Manager row of the RMACCESS table, then there could be data loss on the Tivoli Storage Manager server.

Requirements for using content encryption with Tivoli Storage Manager

To use the content encryption feature, your system must meet the following requirements:

- For each affected Tivoli Storage Manager server, you must set up the TSM client API options files (dsm.opt for Windows and dsm.sys for other operating systems) for encryption.
- You must use the password prompt method for encryption, where a password is delivered to the Tivoli Storage Manager server. You cannot use the password generate method, where Tivoli Storage Manager creates and holds the password for encryption.
- For each resource manager that is going to store data with Tivoli Storage Manager encryption, you must enable the Tivoli Storage Manager encryption feature and supply a passphrase.

Types of data that can be stored with content encryption

If you enable the content encryption feature, you can use it to encrypt new data only. There is no method to encrypt data that was previously stored to the Tivoli Storage Manager server.

The encryption of data applies only as the data is stored to the Tivoli Storage Manager server. Staged data from Tivoli Storage Manager servers is stored in the resource manager staging area as unencrypted data.

Related tasks

Configuring Tivoli Storage Manager for content encryption

Configuring a lockout for resource manager logon failures

You can configure a lockout on the resource manager that prevents an administrator from logging on to that resource manager after a failed number of logon attempts.

When you perform administrative functions on a resource manager, you must log on to that resource manager as the resource manager user. The default behavior of IBM Content Manager is to allow unlimited logon attempts to the resource manager. To prevent an unlimited number of logon attempts, you can configure a lockout on the resource manager. The lockout designates the maximum number of failed logon attempts and sets the duration of the lockout.

The lockout options are set with the following parameters in the RMCONFIGURATION resource manager table.

Table 10. Parameters to set the logon lockout on the resource manager

Parameter name	Definition	Default value
ALLOWED_LOGON_FAILURES	An integer value that is the number of allowed sequential logon failures. After this value is reached, all logon attempts are denied. A value of -1 means that an infinite number of invalid logon attempts is acceptable. The valid range is -1 to 32767.	-1
SEQUENTIAL_LOGON_FAILURES	A nonnegative integer value that is the current count of sequential logon failures. This count increments by 1 until a valid logon resets the value to 0. The value is also set to 0 when the time in LOGON_LOCKOUT_DURATION is reached.	0
LOGON_LOCKOUT_DURATION	A nonnegative integer value in minutes that the lock duration applies. A value of 0 means that no lock duration is set. The valid range is 0 to 32767.	0
LOGON_LOCKED	The parameter to enable or disable the logon lockout. Valid values are true or false.	false

When the resource manager starts, it adds the parameters to the resource manager RMCONFIGURATION database table if they do not exist and sets the values to the defaults so that no lockout is configured. If you want to configure the lockout, you must manually change the values in the RMCONFIGURATION database table.

To configure the lockout:

1. Stop the resource manager application server.
2. Edit the resource manager RMCONFIGURATION database table.
3. Change the value for the **ALLOWED_LOGON_FAILURES** to a non-negative value to designate the number of allowed sequential logon failures.
4. Change the value for the **LOGON_LOCKOUT_DURATION** to the amount of time (in minutes) that you want the login lockout to last. After the lockout duration ends, a user is allowed to attempt to log in to the resource manager again.
5. Start the resource manager again.

Releasing the resource manager lockout

When the resource manager lockout for a defined number of failed logon attempts is set, the resource manager becomes locked for administrative access after that number is reached. There are several ways to release the lockout.

If you attempt to log on to the resource manager with the resource manager user name when the login lockout is in effect, you receive an error message. You must release the lockout so that you can log in to perform administrative tasks on the resource manager.

Tip: You cannot monitor the status of the resource manager lockout by viewing the parameters in the resource manager RMCONFIGURATION database table. The parameters in this table are not updated dynamically as the status changes. They are updated only when a successful logon to the resource manager occurs.

To release the resource manager lockout, choose one of the following options:

Option	Description
Wait until the lockout is released.	The LOGON_LOCKOUT_DURATION parameter in the resource manager RMCONFIGURATION table determines how long the lock on the resource manager lasts. You can wait until the lock is released and then attempt to log on again.
Modify the RMCONFIGURATION parameters to reset the lock.	The value of the LOGON_LOCKED parameter is set to true when the lock is triggered. You can edit the database table to change the value of this parameter to false to release the lock.
Restart the resource manager.	A restart of the resource manager resets the value of the SEQUENTIAL_LOGON_FAILURES parameter to 0 and resets the value of the LOGON_LOCKED parameter to false.

Connecting the system administration client to the databases

You can use the system administration client to connect to various content management databases.

The system administration client in IBM Content Manager can connect to multiple library servers, each of which can connect to multiple resource managers. In IBM Information Integrator for Content, the administration client can connect to multiple administration databases. Although their specific functions are different, the IBM Content Manager library server and the IBM Information Integrator for Content administration database are both system administration databases and the configuration requirements are the same for both.

If you install a system administration database on the same server where you install the system administration client, the information required to connect the local system administration client and the local system administration database is automatically stored in a database connection parameter file. You do not have to perform any post-installation configuration and can connect immediately by logging into the system administration client.

If you install a system administration database on a remote server, you must set up a connection between that server and every system administration client you want to access it from.

Related concepts

“System administration client” on page 106

Related reference

“System administration client logon fails” on page 584

Connecting to a remote database

If you want to connect the system administration client to a remote database, you must first define a connection between the system administration client and the remote database. If you use the system administration client on multiple computers, you must define connections between each system administration client and each remote database.

If you plan to administer both IBM Content Manager and IBM Information Integrator for Content from the same system administration client, and they share a remote database, you only need to define the connection once. If you want to be able to use either the IBM Content Manager system administration client or the IBM Information Integrator for Content administration client with a remote database, you must define the connection in both places. You only need to catalog it once, however. If you have stand-alone remote databases, you must set up each database catalog connection separately.

There are two ways to set up your system administration client to connect to a remote database:

- Use a tool to create the configuration:
 1. Gather information about the remote database.
 2. Use the server configuration utility to set up the connection.

- Manually create the connection:
 1. Gather information about the remote database.
 2. For DB2 databases only, catalog the remote node and database:
 - Databases on z/OS
 - Databases on UNIX or Windows
 3. For Oracle databases only, update the local `tnsnames.ora` file to include the remote database.
 4. Add the connection information to the database connection parameter file. There are separate database connection parameter files for IBM Content Manager and IBM Information Integrator for Content.

Product	Filename
IBM Content Manager	<code>cmbicmsrvs.ini</code>
IBM Information Integrator for Content	<code>cmbds.ini</code>

Related tasks

“Locating the connection parameter file” on page 585

Locating the remote database connection information

You must know the database names and the connection port number to configure a connection between the system administration client and a remote database.

To find the connection information for an Oracle database, view the `oracle_home\network\admin\tnsnames.ora` file in a text editor. This file contains information about the database and is located in the Oracle installation directory, `oracle_home`, on the remote server.

To find the connection information for a DB2 database:

1. Log in to the remote server with a user ID that has DB2 administrative authority.
2. Open a DB2 command prompt.
3. At the DB2 command prompt, enter:


```
list db directory
```

A list of the local and remote databases displays. Local databases are labeled *indirect*.

4. Locate the name of the administration database you want to connect to. Make a note of the DB2 instance that the database is installed on, because different instances can have different connection port numbers.
5. Enter:


```
connect to database user userID using password
```

DB2 connects to the database.

6. Enter:


```
list db tables
```

A list of database tables, and the schema name associated with each table, displays.

7. Make a note of the database schema name, which is required by the server configuration utility.

8. Enter:

```
list node directory
```

Node names and other data for all databases installed or defined on the remote server display.

9. Locate the connection port number associated with the remote system administration database.

Attention: The procedure for identifying the port number varies by operating system. Choose the procedure for the operating system that the remote database is on.

Locating the DB2 connection port number on UNIX

To locate the server name and port number:

1. Open a command prompt.
2. Enter `cd /usr/etc`.
3. Enter `cat services`.
4. Scroll through the list of services until you find the connection port number for the database instance of the remote database. The instance name is usually listed as a comment. If it is not listed, complete the following steps to find the port:
 - a. Open a DB2 command prompt.
 - b. At the DB2 command prompt, verify that you are on the correct instance:

```
get instance
```

DB2 reports the current instance.

- c. Run the following command to find the service name for your instance:

```
get dbm cfg | grep SVCE
```

DB2 reports the service name. For example:

```
TCP/IP Service name          (SVCENAME) = db2cdb2inst24
```

- d. Use the service name to find the port number in the services file. For example, enter a command similar to this one:

```
grep service_name /etc/services
```

DB2 returns the information. For example:

```
service_name  50012/tcp      # Connection port for DB2 instance instance
```

Locating the DB2 connection port number on Windows

To locate the server name and port number on Windows:

1. Open the DB2 Control Center on the remote Windows server.
2. Right-click one of the available instances for the local machine.
3. Click **Setup Communications**.
4. Click **Properties**. The port number is listed in the Properties window.

Locating the DB2 connection port number on z/OS

To locate the server name and port number:

1. Connect to the z/OS system.
2. Issue the `-DISPLAY DDF` command. The `TCPPORT` value in the results is the port number.

Using the server configuration utility

The server configuration utility prompts you for information that enables connectivity between the system administration client and a system administration database. The utility copies the values you enter about the remote system administration database, such as database name, schema name, and so forth, to the database connection parameter file. The database connection parameter file stores the connection parameters that the system administration client needs to connect to the remote database.

You can use the server configuration utility to connect to remote databases.

Instructions for starting the server configuration utility vary by operating system. Once you have started the utility, however, the fields are the same on all operating systems.

You can use the server configuration utility to view existing connections. Click **View Connection Information** to see information on all remote servers configured for use with the system administration client.

After you have added remote database connections with the server configuration utility, you will be able to connect to those servers from the system administration client. The system will automatically catalog the remote database on the first connection.

Restriction: The server configuration utility runs on the system where the system administration client is installed. You use information about the server you plan to connect to when completing the fields.

Running the server configuration utility on UNIX

To start the server configuration utility:

1. Log onto the server as the root user or with a user ID that has write access to all .ini files in the *IBMCMROOT* path.
2. If you access the system administration client from a remote server, export the display. If necessary, modify the xhost settings to allow remote servers to log on to your server.
3. Open a command prompt and change to *IBMCMROOT/config*.
4. Enter `./cmcfg81.sh` to start the server configuration utility.
5. Type the information in the fields. See the explanation of server configuration utility fields for specific field information.
6. Click **OK** to save the configuration.

Related reference

"Finding IBMCMROOT" on page 571

Running the server configuration utility on Windows

To start the server configuration utility on a Windows server:

1. Start the appropriate version of the configuration utility from the Windows Start menu. The server configuration steps are the same for both IBM Content Manager and IBM Information Integrator for Content. You must, however, use the appropriate version of the configuration utility because they save the configuration information in different locations.

Product	Menu selection
IBM Content Manager	Start > IBM Content Manager Enterprise Edition > Server Configuration
IBM Information Integrator for Content	Start > Programs > IBM Information Integrator for Content > Server Configuration Utility

2. Provide the required information in the fields. See the explanation of server configuration utility fields for specific field information.
3. Click **OK** to save the configuration.

Server configuration utility fields

The server configuration utility uses the same fields on all supported operating systems.

Table 11. Field descriptions

Field	Information	Notes
Server type	Select the database type, either IBM Content Manager or IBM Information Integrator for Content .	Tip: You can use the system administration client to manage both database types only if your system includes IBM Content Manager and IBM Information Integrator for Content system administration clients on the same machine.
Server name	Type the alias name of the database you are connecting to. Requirement: You must use the same alias name defined when the database was catalogued.	An alias provides a unique name that identifies the remote database on your workstation. Alias names have an eight-character limit. For example, if the remote database name is ICMNLSDB, an alias could be REMOTE1.
Server repository type	Select the option appropriate for your database and preferred connection method from the list.	For a DB2 database, select DB2 or DB2CON . For an Oracle database, select ORACLE or ORACON . The options anticipate that users will have connection privileges under their own user IDs. If they do not, the connection is eventually made using the shared connection ID. To have users automatically use the shared connection ID when logging in, select DB2CON or ORACON . Important: DB2CON and ORACON are not supported in the cmbicmsrvs.ini file that is used by the system administration client.
Schema name	Type the schema name assigned when the remote database was created.	The default schema name is ICMADMIN.
Host name	Type the name of the computer where the remote database was installed.	Provide the fully qualified host name or IP address of the computer where the remote database is installed.
Operating system	Select the operating system from the list.	Select the operating system in use on the server where the database is located.
Port number	Type the port number assigned to the remote database.	The default connection port number for databases installed on AIX, Linux, Solaris, or Windows is 50000. For z/OS, it is 446.

Table 11. Field descriptions (continued)

Field	Information	Notes
Remote database name	Type the name of the remote database. Use capital letters.	ICMNLSDDB is the default name for the IBM Content Manager and IBM Information Integrator for Content databases.
Node name	Type the node name of the remote database.	The node name is a unique name assigned to the remote database, similar to the alias name you create for the remote database.
Enable single sign-on	Select if single sign-on was enabled during database installation.	The default setting is unchecked (disabled).
Security options	Select Client Authentication if that option was selected during database creation.	The default setting is Server.
User ID	Enter the shared connection user ID.	The default shared connection user ID is ICMCONCT.
Password	Enter the password for the shared connection user ID.	

Manually connecting to a remote DB2 database

If you prefer not to use the server configuration utility, you can use the following procedure to connect the system administration client to a remote DB2 database:

1. Catalog the database either from the command line or using DB2 Configuration Assistant.
2. Update the database connection parameter file with the connection information.

Cataloging the remote database using DB2 Configuration Assistant

To catalog the remote database using DB2 Configuration Assistant, you must know:

- The remote server host name
- The database name
- The database instance port number
- An alias for the remote database, which must be unique on the local system

1. Log in to the system where the system administration client is installed. You must log in with a user ID that has DB2 administration privileges.
2. Open the DB2 Configuration Assistant.

UNIX Use the **db2ca** command.

Windows

The default menu location is **Start > Programs > IBM DB2 > Set-up Tools > Configuration Assistant**.

3. Follow the DB2 Configuration Assistant prompts to catalog and test the connection to the remote database. See the DB2 Configuration Assistant help or the Configuration Assistant topic in the DB2 Universal Database Information Center for more information.

If the DB2 Configuration Assistant connection test was successful, use the server configuration utility to finish adding the remote database.

Related information

 DB2 Configuration Assistant

Cataloging a remote node and database on UNIX or Windows

Tip: You can also use the DB2 Configuration Assistant to catalog the database.

To catalog a remote database located on a UNIX or Windows server, complete the following steps. See the descriptions of node and database cataloging variables for additional information.

1. Open a DB2 command prompt on the system where the system administration client is installed.
2. At the DB2 command prompt, enter the following command to catalog the remote node:

```
catalog tcpip node nodename remote remote_hostname  
server port_number with \"your comments\"
```

For example:

```
catalog tcpip node nodesun5 remote hostname.svl.ibm.com server 50000  
with \"remote node sun5\"
```

3. Enter the following command to display a list of nodes:

```
list node directory
```
4. Check to see that the new node is included in the list, and that the node name and port number are correct. If the node is included, continue on to the next step.
5. Enter the following command to catalog the remote database:

```
catalog db remote_database_name as local_alias_database_name  
at node nodename
```

For example:

```
catalog db icmnlbdb as remotel at node nodesun5
```
6. Enter the following command to display a list of databases that are cataloged on the local system:

```
list db directory
```
7. Check that the new database is included in the list. Verify that the node name, database name, and alias name are correct. If the database is included, then the cataloging is complete.

After you have cataloged the remote node and database, you must add the connection information to the database connection parameter file.

Cataloging a remote node and database on z/OS

Tip: You can also use the DB2 Configuration Assistant to catalog the database.

To catalog a remote database located on a z/OS server, complete the following steps. See the descriptions of node and database cataloging variables for additional information.

1. Open a DB2 command prompt on the system where the system administration client is installed.
2. At the DB2 command prompt, enter the following command to catalog the remote node:

```
catalog tcpip node nodename remote tcpip_address server port_number
```

For example:

```
catalog tcpip node mvsnodel remote 10.0.0.1 server 446
```

3. Enter the following command to display a list of nodes:

```
list node directory
```

4. Enter the following command to catalog the database as a Database Connection Service (DCS) database:

```
catalog dcs database remote_database_name as remote_database_name
```

For example:

```
catalog dcs database icmnlbdb as icmnlbdb
```

5. Check to see that the new node is included in the list, and that the node name and port number are correct. If the node is included, continue on to the next step.

6. Enter the following command to catalog the remote database:

```
catalog db remote_database_name as local_alias_database_name  
at node nodename
```

For example:

```
catalog db icmnlbdb as remotel at node mvsnodel
```

7. Enter the following command to display a list of databases that are cataloged on the local system:

```
list db directory
```

8. Check that the new database is included in the list. Verify that the node name, database name, and alias name are correct. If the database is included, then the cataloging is complete.

9. Bind your client against the database you just cataloged. The typical format for a bind command is:

```
bind @listname
```

See the DB2 Universal Database Information Center for information about binding databases.

After you have cataloged the remote node and database, you must add the connection information to the database connection parameter file.

Related information

 [BIND command](#)

Node and database cataloging variables

The following list defines the variables used when you catalog the remote node and database.

local_alias_database_name

The new database name on your local machine. It must be different from all other alias database names on the local system.

nodename

A name you assign to identify the node.

port_number

The remote server name, or the port number of the remote server database manager instance.

remote_database_name

The real database name on the remote system that you want to catalog on your local machine.

remote_hostname

The fully-qualified remote host name, for example, hostname.svl.ibm.com.

tcpip_address

The TCP/IP address of the remote server.

your comments

Comments you want to save. You must use a backslash followed by a quotation mark both before and after the comment string to permit spaces. For example:

\ "This is a comment.\ "

Database connection parameter file

To edit the database connection parameter file, use any text editor. Always make a backup copy before editing the file.

Product	Filename
IBM Content Manager	cmbicmsrvs.ini
IBM Information Integrator for Content	cmbds.ini

cmbicmsrvs.ini parameters

The following list defines each parameter in the cmbicmsrvs.ini file, the file that defines the connection parameters between the IBM Content Manager system administration client and the library server.

Important: For all parameters in the cmbicmsrvs.ini file, you can also provide a value in the connect_string parameter of the DKDatastoreICM::connect method. A value in the connect_String parameter takes precedence over a value in the cmbicmsrvs.ini file.

ICMSERVER

Type the database name. The default name is ICMNLSDB.

If you are connecting to multiple remote databases, you must catalog each remote database before you add an entry to the cmbicmsrvs.ini file. If you are connecting to multiple local and remote databases that are all named ICMNLSDB, type an alias name in this field. An alias provides a unique name that identifies the remote database on your workstation. Alias names have an eight-character limit. For example, if the remote database name is ICMNLSDB, an alias might be REMOTE1.

ICMSERVERREPTYPE

Type the option that matches your database and connection preference in this field. The value for this parameter must be in all uppercase characters.

DB2 Users connect to DB2 by using the privileges associated with their own user IDs, if possible. If the user ID does not have the correct privileges, the connection is made with the shared connection ID.

DB2CON Users connect to DB2 by using the shared connection ID.

Important: DB2CON is not supported in the cmbicmsrvs.ini file that is used by the system administration client.

ORACLE Users connect to Oracle by using the privileges associated with

their own user IDs, if possible. If the user ID does not have the correct privileges, the connection is made with the shared connection ID.

ORACON Users connect to Oracle by using the shared connection ID.

Important: ORACON is not supported in the cmbicmsrvs.ini file that is used by the system administration client.

ICMSchema

Type the schema name that was assigned to the database during installation. If you do not know the schema name, see the information about connecting the administration client to databases. The default schema name is ICMADMIN.

ICMSSO

If single sign-on was enabled when the database was created, type TRUE. If single sign-on was not enabled, type FALSE. The default setting is FALSE.

ICMDBAUTH

Specify where the user ID authentication takes place. If user authentication occurs on the server where the database is installed, type SERVER. If authentication occurs on the client, type CLIENT.

ICMREMOTE

Specify whether the server is remote. Type TRUE for a remote server or FALSE for a local server.

ICMHOSTNAME

Type the host name of the server where the database that you want to connect to is installed. Depending on your company's network configuration, you can type either an IP address or a domain name.

ICMPORT

Type the port number assigned to the database during installation. The default connection port number for databases installed on AIX, Linux, Solaris, or Windows is 50000. For z/OS, it is 446.

ICMREMOTEDB

Type the name of the database that was assigned during installation. The default name is ICMNLSDB.

ICMNODENAME

Type the name of the node.

ICMOSTYPE

Type the name of the operating system on the server where the database is installed.

AIX For AIX

LINUX For Linux

SUN For Solaris

WIN For Windows

OS390 For z/OS

ICMJDBCdriver

Type the Java Database Connectivity (JDBC) driver name.

ICMJDBCURL

Type the JDBC URL.

ICMJNDIREF

Type the Java Naming and Directory Interface (JNDI) indirect lookup resource reference string for the WebSphere Application Server connection pool. This string is used when a connection is requested with the JNDI indirect lookup.

ICMDBVER

For an Oracle database, type the database version used on the client side.

10 For Oracle Database 10g.

11 For Oracle Database 11g.

The C++ API requires this value to use the correct archive libraries and compiler. If no value is specified, the default value is 10. This parameter is not used by a DB2 database.

ICMGMTSYSATTRTS

Specify whether to use Greenwich mean time (GMT) for the following system attributes: SYSROOTATTRS.CREATETS, SYSROOTATTRS.LASTCHANGEDTS, and SYSROOTATTRS.CHKOUTTIMESTAMP. Type TRUE to use GMT. If no value is specified, the default value is FALSE.

cmbds.ini parameters

The following list defines each parameter in the cmbds.ini file, which defines the connection parameters between the IBM Information Integrator for Content system administration client and the administration database.

FEDSERVER

Type the database name. The default name is ICMNLSDB.

If you are connecting to multiple remote databases, you must catalog each remote database before you add an entry to cmbds.ini. If you are connecting to multiple local and remote databases that are all named ICMNLSDB, type an alias name in this field. An alias provides a unique name that identifies the remote database on your workstation. Alias names have an eight-character limit. For example, if the remote database name is ICMNLSDB, an alias might be REMOTE1.

FEDSERVERREPTYPE

Type the option that matches your database and connection preference in this field. The value for this parameter must be in all uppercase characters.

DB2 Users connect to DB2 by using the privileges associated with their own user IDs, if possible. If the user ID does not have the correct privileges, the connection is made with the shared connection ID.

DB2CON Users connect to DB2 by using the shared connection ID.

ORACLE Users connect to Oracle by using the privileges associated with their own user IDs, if possible. If the user ID does not have the correct privileges, the connection is made with the shared connection ID.

ORACON Users connect to Oracle by using the shared connection ID.

FEDSCHEMA

Type the schema name that was assigned to the database during

installation. If you do not know the schema name, see the information about connecting the administration client to databases. The default schema name is ICMADMIN.

FEDSSO

If single sign-on was enabled when the database was created, type TRUE. If single sign-on was not enabled, type FALSE. The default setting is FALSE.

FEDDBAUTH

Specify where the user ID authentication takes place. If user authentication occurs on the server where the database is installed, type SERVER. If authentication occurs on the client, type CLIENT.

FEDREMOTE

Specify whether the server is remote. Type TRUE for a remote server or FALSE for a local server.

FEDHOSTNAME

The host name of the server where the database that you want to connect to is installed. Depending on your company's network configuration, you can type either an IP address or a domain name.

FEDPORT

Type the port number assigned to the database during installation. The default port number is 50000.

FEDREMOTEDB

Type the name of the database that was assigned during installation. The default name is ICMNLSDB.

FEDNODENAME

Type the name of the node.

FEDOSTYPE

Type the name of the operating system on the server where the database is installed.

AIX For AIX

LINUX For Linux

SUN For Solaris

WIN For Windows

OS390 For z/OS

FEDJDBCDRIVER

Type the Java Database Connectivity (JDBC) driver name.

FEDJDBCURL

Type the JDBC URL.

Related tasks

“Locating the connection parameter file” on page 585

Related reference

“Finding IBMCMROOT” on page 571

Developing federated searches with IBM Information Integrator for Content

Most of the time, client application users do not want to search for information on a server-by-server basis. Instead, they want to conduct a single federated search, where they can search multiple content servers at once.

With IBM Information Integrator for Content, you can create search templates for federated searches. Because each content server stores and organizes information differently, the search template must account for these differences for each server. Before you create the search template, you must first create federated entities, which map their attributes to native attributes on content servers.

Creating federated searches involves the following tasks:

- Defining connections to content servers using IBM Information Integrator for Content connectors.
- Creating federated entities by:
 - Creating federated attributes
 - Mapping federated attributes to native attributes
 - Defining federated entities
 - Assigning parameters
- Creating search templates by:
 - Defining the search template
 - Defining search criteria
 - Defining template settings
 - Assigning access to client users

Mapping native and federated data

You can perform these tasks manually or using wizards.

Creating a federated entity with the wizard

The Create Federated Entities wizard enables you to obtain a server inventory that can be filtered on content servers. Filtering is not an option if you use the manual (nonwizard) method to create a federated entity. The Federated Entity wizard also generates valid default parameters for federated attributes, which reduces the chance of incorrectly configuring them.

The Create Federated Entity wizard includes a server inventory that can be filtered to make finding native attributes easy. A server inventory lists all of the native entities and their native attributes, from which you can select the native attributes you want to use in your federated entity.

When you define native attribute properties, you cannot make them more restrictive than the properties already defined by the native attributes mapped to the federated attribute. The wizard provides default properties that meet this criterion. If, after you have customized the default properties for the default federated attribute, you want to revert to the default properties suggested by the wizard, you can.

When you create a federated entity, you:

1. Name and describe the federated entity. You can also determine whether you want the federated entity to be text-searchable.
2. Define the federated attributes.
3. Map federated attributes to native attributes. Tools are provided to obtain a server inventory, to select the native attributes you want to map, and to modify your mappings at a later date.
4. Choose native attributes that share properties so that you can create a usable federated attribute.

Begin to create a federated entity by completing the following steps:

1. In the navigation pane, right-click **Federated Entities > Wizard**. The Federated Entity Wizard window opens.
2. Enter a descriptive name for the federated entity. You cannot use spaces or single quotation marks. Federated entity names must be unique.
3. Enter up to 254 characters describing the new federated entity in the **Describe the federated entity** field. For example, if you create a federated entity for employee information that includes employee IDs and their salaries, you can name your federated entity `Employee_Info`. In the description field, you can type: `Contains employee IDs and employee salaries`.
4. Optional: Select **Make this entity text searchable** if users need to conduct searches across several content servers that contain information that pertains to the federated entity. If you do not enable text search for the federated entity, then users must wait a long time for the search results to return.
5. Optional: Select **Create a native federated folder to store this federated entity** to store native entities in a federated folder.
6. Click **Next** to proceed on to the next step, or, you can click a specific tab.

Attention: Be aware that when you are using the wizard to create a federated entity on the Map Federated Attributes page, and click **Map**, you might receive the following error:

Mapping is invalid. Native attribute parameters cannot be more restrictive than the federated attribute parameters.

This error appears when you attempt to map native attributes from multiple content servers. You can work around this error by creating this federated entity manually. From the system administration client navigation pane, right-click **Federated Entities** and click **New > Nonwizard**.

Adding a federated attribute with the wizard

To add a federated attribute to a federated entity, complete the following steps:

1. Enter a descriptive name for the federated attribute. You cannot use spaces or single quotation marks in the name, and it must be unique.
2. Optional: If you want to modify an existing attribute, select its name from the table.
3. Enter up to 254 characters describing the attribute in the **Describe the federated attribute** field.

For example, if you create a federated entity called `Employee_Info` that contains employee IDs and employee salaries, you can create two federated attributes, one called `Employee_ID` and another called `Salary`. You can describe `Employee_ID` as contains employee identification numbers and `Salary` as contains employee base salary information.

4. Click **Add** to include the federated attribute in the **Federated attributes** table. Any federated attributes that you create for this federated entity display in the **Federated attributes** table. To remove a federated attribute from a federated entity, select it from the **Federated attributes** table and click **Delete**. Deleting the federated attribute removes it completely from the IBM Content Manager server.
5. Click **Next** to proceed on to the next step, or, you can click a specific tab.

Mapping to one or more native attributes with the wizard

During a search, users can retrieve only native attributes that have a mapped federated attribute.

To map a federated attribute with a native attribute, complete the following steps:

1. Select a federated attribute from the list. The list contains all of the federated attributes that you created and saved on the IBM Content Manager server. If you do not see a federated attribute that you want to use, you must define it on the previous page, Define Federated Attributes.
2. Select a content server that you want to map to. Selecting **All Servers** returns any server that is defined in the IBM Content Manager system administration client.
3. Select the native entity that contains the native attribute that you want to map with the federated attribute. If you select **All Servers** and **All Native Entities**, you can view all of the native entities on all of the content servers. If you select **All Servers** and one native entity name, you might find that this native entity name exists on more than one server. You can continue to narrow your choices by selecting a specific content server and native entity.
4. Select a data type that is common to the native attributes that you want to map. If you map native attributes that are vastly different from each other, trying to define federated attribute properties can pose problems. For example, if a value for one native attribute is a character and the other is a long integer, you cannot define a common data type for the federated attribute for these two native attributes.
5. Optional: Click **Filter Native Entities** to constrain the list of native entities in the list. If you previously filtered objects, the first item listed under **Native Entity** is **Click on Filter**. Follow these steps to create or change your entity filter.
 - a. Click **Filter Native Entities** to open the Filter Native Entities window.
 - b. Depending on the entities that you want to display, select **Only show native entities** and enter the filter information. IBM Content Manager displays the entities that match your filter information.
 - c. Click **OK**.
6. Click **Retrieve Server Inventory** to populate the table with your search results.
7. Select one or more native attributes from the search results to map with the federated attribute. If you do not see the native attributes that you want, reset the filters to search a larger area.
8. Click **Map**. Your selections display in the **Mapped attributes** table. Click **Remove** to remove any native attributes that you do not want to map to your federated attribute. Clicking **Remove** does not delete the native attributes from their native servers.
9. Click **Next** to proceed on to the next step, or, you can click a specific tab.

Defining the properties of a federated attribute with the wizard

You must define properties for the federated attribute. You define federated attribute properties by assessing the properties of the native attributes that you mapped to the federated attribute. Then you select the common data types between the native attributes.

If native attributes do not have common data types, any attempts at using the federated entity results in failure. Return to the previous section, “Mapping to one or more native attributes with the wizard” on page 81, and map attributes that have common data types.

To define federated attribute properties, complete the following steps:

1. Select a federated attribute from the list. Only those attributes that you defined for this federated entity display in the list.

The **Mapped native attributes** table displays all of the native attributes mapped to the federated attribute that you select from the list. In the table, you can see the native attribute properties. You can select the appropriate data types and data type properties for the federated attribute. If the data types and data type properties of the native attributes mapped to the federated attribute vary widely, then you must return to “Defining the properties of a federated attribute with the wizard,” and select native attributes that share data types and data type properties.

2. Select a data type from the **Data type** list. Depending on what you select as the data type, the fields for **Length**, **Precision**, **Scale**, **Minimum**, and **Maximum** become active.

IBM Information Integrator for Content displays any common properties. For example, if all of the native attributes share a length of 10, when you choose VarChar as the data type, IBM Content Manager inserts 10 into the **Length** field. You can change any supplied default value.

3. Click **Define** to set the federated attribute properties.

If you want to change the properties later, you can use the wizard to change these properties.

Modifying an existing federated entity with the wizard

To modify an existing federated entity, select any tab and change the properties. You can change any field. Changes do not take effect until you click **Define** on the Define properties page or until you click **Finish**.

To modify an existing federated entity, complete the following steps:

1. In the navigation panel, right-click **Federated Entities > wizard**. The Federated Entity Wizard window opens.
2. Optional: Enter a descriptive name for the federated entity. Enter any further explanation of the new federated entity in the **Describe the federated entity** field. For example, if you create a federated entity for employee information that includes employee IDs and their salaries, you can name your federated entity Employee_Info. In the **Description** field, you can type: Contains employee IDs and employee salaries.
3. Optional: Select **Allow text searching with this federated entity** if users must conduct searches across several content servers that contain information that pertains to the federated entity. If you do not enable text search for the federated entity, then users will have to wait a long time for the search results to return.

Tip: You cannot create a useful search template without enabling text search.

Creating a federated entity manually

Use the New Federated Entity window to define a federated entity and map the federated attributes to the native attributes. You create federated entities for use in search templates. When a search runs, IBM Content Manager uses the associated federated entity's federated attributes to search the native attributes and return with the result.

Restriction: After you save a federated entity, you cannot remove or modify any of its attributes or change its description, but you can continue to add attributes, add mappings, or remove mappings.

Requirement: Before you can create a federated entity, you must refresh the server inventory for all of the content servers to ensure that they have the most recent collection of native entities and native attributes. You must also create attributes first, and you can create them from the New Federated Entity window.

To create a federated entity, complete the following steps:

1. In the navigation pane, right-click **Federated Entities** and click **New > Nonwizard**. The New Federated Entity window opens.
2. Enter a name for the federated entity in the **Name** field. You cannot use a forward slash (/) in the name. When you name your federated entity, consider the native entities that you want to map to it. Find a common theme among the native entity names and assign a name to your federated entity that reminds you of the native entities that you mapped to it.
3. Optional: Enter a description for the federated entity in the **Description** field. You might want to describe the native entities or content servers you mapped to this federated entity. If the native entities are not similar, consider writing a description to remind you of the native entities that you included in the federated entity.
4. Optional: Select **Text Searchable** if users need to conduct text searches across several content servers. If you do not enable text search for the federated entity, then users must wait a long time for the search results to return.
5. Optional: Select **Create a native federated folder to store this federated entity** to store native entities in a federated folder.
6. Optional: Click **Add** to open the New Federated Attribute window where you can create additional federated attributes. You can associate a federated attribute with only one federated entity, but a federated entity can contain more than one federated attribute.
7. Click **Map Federated Entity** to open the Federated Entity Mapping window. In this window, you can map the federated entity and its federated attributes to the native entities and their native attributes for the content servers that you defined.
8. Click **OK** to save the federated entity and close the window.

Refreshing the server inventory

You must refresh the server inventory to gather the native entities and native attributes on each content server before you can create the federated attributes. After you refresh the server inventory, you can view it in the Server Inventory Viewer window.

To refresh the server inventory, complete the following steps:

1. Click **Servers** in the tree view to show the defined content servers in the right pane. Right-click a server name and click **Refresh Server Inventory**. The Information Message window opens.
2. Click **Yes** to run the server inventory. If your IBM Content Manager user ID is not already mapped to your user ID on the content server, you are prompted for your user ID and password for the content server.
If user mapping is turned on, IBM Content Manager saves the content server user ID and password associated with your IBM Content Manager user ID and password for future connections.

Filtering the server inventory:

You can filter the list of native entities that display in the Server Inventory Viewer window. Limiting the display to specific entities might make finding entities easier and saves processing time.

To view the server inventory, click **Tools > Server Inventory Viewer** from the menu bar. The Server Inventory Viewer filter window opens, so you can first filter the objects that display.

1. Select one of the following choices:
 - **Show all native entities:** Selecting this button displays all of the native entities. You can use this choice to reset the filtering to its pre-filtered state.
 - **Only show native entities:** Selecting this button enables you to filter the display by choosing specific text to look for:
2. If you selected **Only show native entities**, select how to filter the objects:
 - Starting with
 - Containing
 - Ending with

Specify the text to filter. Do not include wildcard characters or spaces.
3. Click **OK**.

The system administration client saves the options you select and remembers them for the next session. To change the filtering options, you can select **Tools > Server Inventory Viewer** from the main menu.

Viewing server inventory logs:

Use the Log Viewer window to view the log generated after refreshing the server inventory.

The log shows a list of messages generated when differences are found between the new and previous inventories. For example, changes in the native inventory might affect the existing federated entity mappings and search templates. You then need to review federated entities and search templates to change or remove invalid items.

- To view the log, click **Tools > Log Viewer** from the menu bar. The Log Viewer window opens. The log shows the date, time, and a message for each event found during an inventory update. After you have checked the log, you can clear any old messages.
- To clear entries in the log:
 1. Select the log entries you want to clear.
 2. Click **Edit > Cut**.

3. Click **OK**.
- To clear the entire log:
 1. Click **Edit > Select All**.
 2. Click **Edit > Cut**.
 3. Click **OK**.

Filtering objects from display in IBM Information Integrator for Content:

To limit the retrieval and display of objects that have large volumes, you can filter what you want the system administration client to display.

To filter objects from display, complete the following steps:

1. From the main menu, select **Tools > Filter Objects Options** to open the Filter Objects Options window.
2. Select one or more of the following check boxes:
 - **User**
 - **User groups**
 - **ACL**
 - **Federated Entity**
 - **Search Template**
 - **Server Inventory**

By default, all objects are cleared.

3. Click **OK**.

If an object is selected for filtering, the next time you open a system administration window that displays that object, the Filter *Objects* Options window opens to enable you to define what you want to display.

The system administration client saves the options that you select and remembers them for the next session.

Filter object:

After you select an object for filtering, the next time the system administration client needs to display that object, you are prompted to choose how you want to limit the display of the object. Alternately, you can right-click the object from the system administration tree and select **Filter and Explore**.

1. From the Filter *object* window, you can select one of the following choices:
 - **Show all objects:** Selecting this button displays all of the selected objects
 - **Only show objects:** Selecting this button enables you to further filter the display by choosing specific text to look for:
2. If you selected **Only show objects**, select how to filter the objects:
 - Starting with
 - Containing
 - Ending with

Specify the text to filter. For example, to display only users whose given name is Jane, select **Starting with** and enter Jane in the text field. Do not include spaces or wildcard characters.

3. Click **OK**.

The system administration client saves the options you select and remembers them for the next session. To change the filtering options, you can select **Tools > Filter Object Options** from the main menu.

Creating a federated attribute

Use the New Federated Attribute window to create federated attributes or copy existing federated attributes from another federated entity.

Prerequisite: Run the server inventory for all of the content servers to collect the current native entities and native attributes.

- To create a federated attribute, complete the following steps:
 1. Click **Add** in the New Federated Entity window. The New Federated Attribute window opens.
 2. Click **Add federated attribute** to create a federated attribute.
 3. Enter a name for the federated attribute in the **Name** field. You cannot use a forward slash (/) in the name.
 4. **Optional:** Enter a description for the federated attribute in the **Description** field.
 5. Select the attribute type from the **Enter** list.
 6. Specify the parameter types.

Restriction: When specifying the nullable, queryable, and updatable parameter types, a federated attribute can be more restrictive than a native attribute, but a native attribute cannot be more restrictive than a federated attribute. For example, you can specify **nullable** for both the federated and native attribute. You can also specify **not nullable** for the federated attribute and **nullable** for a native attribute, but not vice versa.

7. If you want to create additional federated attributes, click **Apply** to create the federated attributes and repeat steps 2 through 7. If you are finished creating federated attributes, click **OK** to create the federated attributes and close the window. Clicking **Cancel** closes the window without saving the last attribute that you defined.
- To add an existing federated attribute from another federated entity to this federated entity, complete the following steps:
 1. Click **Add** in the New Federated Entity window. The New Federated Attribute window opens.
 2. Click **Select existing federated attribute**.
 3. Select a federated entity from the **Federated entity** list. The fields are populated with the values defined in the existing federated entity.
 4. Select a federated attribute from the **Federated attribute** list.
 5. Enter a new name for the federated attribute in the **Name** field.
 6. Enter a description for the federated attribute in the **Description** field.
 7. Modify other properties as appropriate.

Restriction: A federated attribute can be more restrictive than a native attribute, but a native attribute cannot be more restrictive than a federated attribute. For example, you can specify **nullable** for both federated attribute and native attribute. You can also specify **not nullable** for a federated attribute and **nullable** for a native attribute, but not vice versa.

8. Click **OK** to create the federated attribute and close the window.

Native attribute:

A *native attribute* is an attribute, or characteristic, that is managed on a specific content server.

You may have similar native attributes on different content servers. Each federated attribute can map multiple native attributes and each native attribute can be mapped from multiple federated attributes.

Viewing or modifying an existing federated attribute:

Use the Federated Attribute Properties window to view or modify a federated attribute.

Prerequisite: Run the server inventory for all the content servers to collect the current native entities and native attributes.

To view or modify a federated attribute, complete the following steps:

1. If you have already mapped a federated attribute, and you want to modify it, you must first remove the mapping by clicking **Map Federated Entity** and removing the federated entity mapping from the **Federated entity mappings** list.
2. In the New Federated Entity window, select a federated attribute from the **Federated attributes** list.
3. Click **Modify**. The Federated Attribute Properties window opens.
4. View or modify the properties in this window. You can modify any of the properties except for the name.
5. Click **OK** to save the changes and close the window.

Viewing native entities and native attributes:

Use the Server Inventory Viewer window to view content servers, native entities, native attributes, and the parameter type values of the native attributes.

To view the native entities and native attributes, complete the following steps:

1. Click **Tools > Server Inventory Viewer** in the System Administration Client window. The Server Inventory Viewer window opens.
2. When you have finished viewing the items listed in the window, click **File > Close**.

Mapping a federated entity

To map a federated entity and its federated attributes to a native entity and its native attributes, complete the following steps:

1. Click **Map Federated Entity** in the New Federated Entity window or Federated Entity Properties window. The Federated Entity Mapping window opens.
2. Select the content server of the native entity from the **Server** list.
3. Select a native entity from the **Native entity** list.
4. Optional: Click **Filter Native Entity** to constrain the list of native entities in the list. If you previously filtered objects, the first item listed under **native entity** is **Click on Filter**. Follow these steps to create or change your entity filter.
 - a. Click **Filter Native Entities** to open the Filter Objects Options window.
 - b. Select **Federated entities** and click **OK**. A filter window opens.

- c. Depending on the entities that you want to display, select **Only show native entities** and enter the filter information. IBM Content Manager displays the entities that match your filter information.
- d. Click **OK**.
5. Select a federated attribute from the **Federated attribute** list.
6. Select a native attribute from the **Native attribute** list.
7. Click **Add** to add the mapping to the **Federated entity mappings** list.
8. Optional: If you want to map additional attributes, repeat steps 2 through 7.
9. Click **OK** to save the mappings and close the window.

Federated entity:

A *federated entity* is an IBM Content Manager metadata object that is comprised of federated attributes and optionally associated with one or more federated text indexes.

Restriction: The federated connector is deprecated.

Every content server has entities and every entity has attributes. Entities are groupings of data stored in a server. For example, relational databases use tables as entities. In IBM Content Manager, the entity is known as an item type and the item type attributes are called attributes. In IBM Content Manager, the entity is known as a federated entity and its attributes are known as federated attributes. In IBM Content Manager, content server entities, like IBM Content Manager item types, are called native entities and the content server attributes are called native attributes.

When you create a federated entity, you map all of its attributes to corresponding native attributes on the content servers that you want to query. Figure 2 shows how the federated attribute `policy_number` in the federated entity `Auto_Claim` can map to more than one native attribute on several content servers.

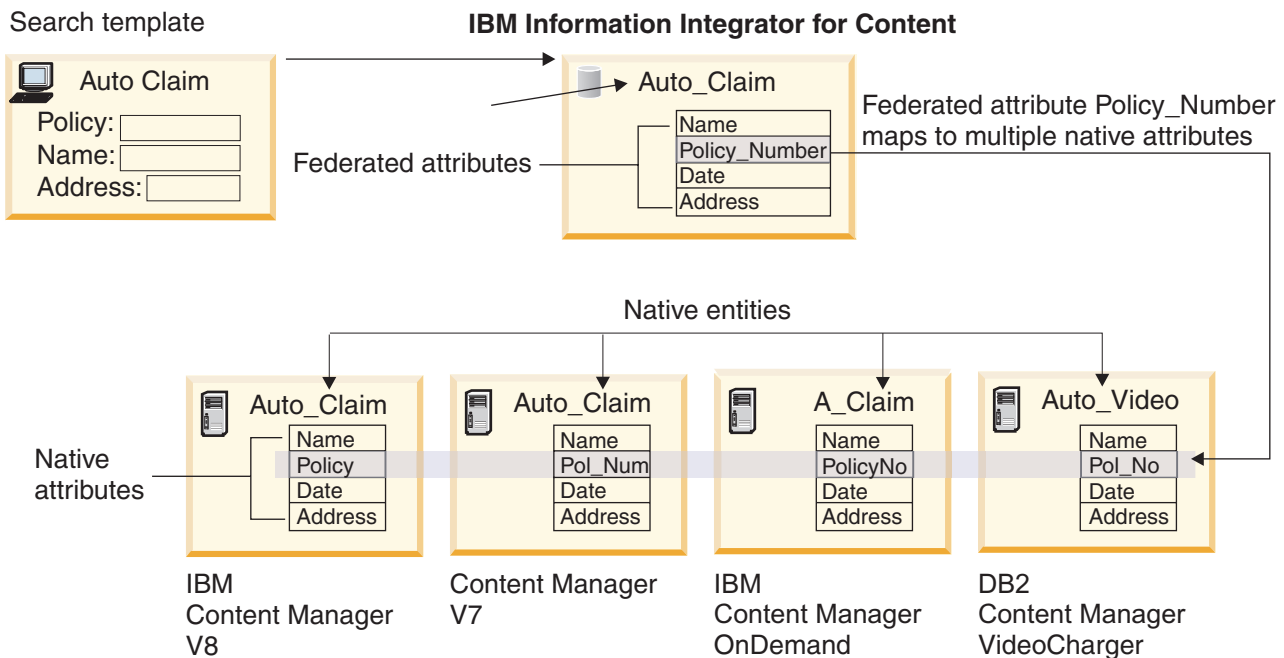


Figure 2. Federated entity has a federated attribute with multiple native attributes associated to it.

IBM Content Manager uses federated entities to search across multiple content servers, retrieve information, and optionally save the search results in federated folders. IBM Content Manager client applications conduct searches using federated entities through search templates. Each search template represents one federated entity. When a search runs, IBM Information Integrator for Content uses the associated federated entity's federated attributes to search the native attributes and return with the result. If you mark the federated entity to act as a folder, the search results, which are locations of objects on content servers, are saved in the federated folder to shorten the wait time if the same search is conducted multiple times.

Federated folder: A *federated folder* is a special-purpose folder used in IBM Information Integrator for Content to store native entities (documents and folders) from one or more content servers. You can store the combined results from a federated query from one or more content servers in a federated folder. A federated folder is a federated entity.

Federated folders are used in workflow. When you create a workflow with collection points, you must use a federated entity that has federated folder properties. You use a federated folder to hold the multiple object locations that you need to complete a workflow. For example, a claim process requires several documents to be approved. You use a federated folder to contain the location of all those documents throughout the workflow claim process. You cannot include collection points in a workflow unless you have defined at least one federated entity that has folder properties.

Native entity:

A *native entity* is an object that is managed on a specific content server and that is comprised of native attributes.

For example, IBM Content Manager index classes are native entities comprised of IBM Content Manager key fields.

Native attributes are objects that are managed on a specific content server and is specific to that content server. For example, the key field policy num might be a native attribute in an IBM Content Manager content server, whereas the field policy ID might be a native attribute in a Content Manager OnDemand content server.

Viewing or modifying an existing federated entity:

Restriction: If you create a federated folder to store this federated entity, you can modify only the description after you save it. You can always delete an existing federated entity, but you must also delete any search templates associated with it.

To view or modify an existing federated entity, complete the following steps:

1. Click **Federated Entities** from the tree view in the Administration window to display the federated entities in the right pane.
2. Right-click a federated entity and select **Properties**. The Federated Entity Properties window opens.
3. View or modify the properties in the window.

Restriction: For an existing federated entity, you can add attributes, and add or remove a mapping, but you can not remove or modify an attribute, or change an attribute description.

4. If you modified any properties, click **OK** to save the federated entity and close the window.

Copying a federated entity:

Copy a federated entity when you want to create a federated entity with similar, or the same, properties.

To copy a federated entity, complete the following steps:

1. Click **Federated Entities** in the tree view in the Administration window to display the federated entities in the right pane.
2. Right-click a federated entity and select **Copy**. The Copy Federated Entity Window opens.
3. Enter a new name in the **Name** field.
4. Modify the properties as appropriate.
5. Click **OK** to save the new federated entity and close the window.

Creating a federated text index

Optional: You can create a federated text index using the New Federated Text Index window. You must have your text search server running to update the server inventory.

To create a federated text index, complete the following steps:

1. From the navigation pane, right-click **Federated Text Indexes** in the tree view and click **New**. The New Federated Text Index window opens.
2. Enter a name for the federated text index in the **Name** field.
3. Optional: Enter a description in the **Description** field. You cannot change the description of a federated text index after the federated text index has been created.
4. Select a text server from the **Text server** list. The native text indexes display in the **Native text indexes** list.
5. Select a native text index from the **Native text indexes** list. The federated text index maps to this native text index on the text server.
6. Click **Add** to add the selected server and index to the **Selected Servers and Indexes** list.
7. Click **Associate Federated Entity** to open the Associate Federated Entity window where you can associate federated text indexes with federated entities. You must associate this federated text index with a federated entity to enable combined searches. After associating the federated entity, you return to the New Federated Text Index window.
8. Click **OK** to save the federated text index and close the window.

Native text index:

A *native text index* is an index of the text items that are managed on a specific content server.

You can create a federated text search index that searches a combination of native text indexes and native attributes.

Associating a federated entity to a federated text index:

Use the Associate Federated Entity window to create an association between federated entities and federated text indexes. The association is required for combined searches of both federated attributes and text indexes.

To associate a federated entity, complete the following steps:

1. Open an existing federated text index from the main system administration window.
2. Click **Associate Federated Entity**.
3. Select an item from the **Selected Servers and Indexes** list.
4. Select a federated entity from **Federated entity** list. The native entities that are mapped to the federated entity display in the **Native entity** list.
5. Select a native entity from the **Native entity** list.
6. Click **Map**. The mapping is added to the **Federated text index mappings** list. If you want to associate another federated entity, you must first remove the item in the **Federated text index mappings** list.
7. Click **OK** to save the mapping and return to the federated text index window.

Viewing or modifying an existing federated text index:

To view or modify an existing federated text index, complete the following steps:

1. Click **Federated Text Indexes** in the tree view in the navigation pane to display the federated text indexes in the details pane.
2. Right-click a federated text index and select **Properties**. The Federated Text Index Properties window opens where you can view or modify all of the properties except the name, description, and associated server.
3. If you have modified properties, click **OK** to save the federated text index and close the window.

Copying a federated text index:

To copy a federated text index, complete the following steps:

1. Click **Federated Text Indexes** in the navigation pane to display the federated text indexes.
2. Right-click a federated text index and select **Copy**. The Copy Federated Text Index window opens.
3. Enter a new name in the **Name** field.
4. Modify the properties as appropriate.
5. Click **OK** to save the new federated text index and close the window.

Search template

Search templates allow client applications to access the federated mappings with content servers. After you create a federated entity, you create a search template. A search template uses a federated entity as a map to where content is stored.

When you create the search template, you must define what you want to search for, what you want to do with the search results, and who has permission to use the template. While you can use a federated entity only once for each template, you can use a single federated entity for multiple templates. You can also search on any combination of the federated attributes as search criteria.

When you create a search template, you must:

- Assign the users and user groups who have access to the search template through their client application
- Define search criteria using the federated attributes in the federated entity.
- Specify the valid and default operators, default values for the criteria, and characteristics of the search results display

You can create a search template in two ways:

- Using the Search Template Wizard
- Using the manual method

Three advantages of creating a search template using the wizard:

- The wizard can help new administrators understand how to create a search template
- Experienced administrators can quickly modify search templates
- You can preview the search template appearance, including how the results display to your users.

Defining a search template with the wizard

The Search template wizard helps you create search criteria. It also helps you design how the search criteria and results displays will look and act. It even provides you with a preview of what the search template might look like in your client application. Additionally, the windows for creating federated entities and search templates for IBM Content Manager are also available for those who prefer them.

Requirement: Before you can create a search template, you must define a federated entity.

To create a search template, complete the following steps:

1. In the system administration tree, right-click **Search Templates > New > Wizard**. The Search Template Wizard window opens.
2. Enter a descriptive name for the search template. The search template name must be unique.
3. Enter any further explanation of the new search template in the **Description** field. For example, if you create a search template to search for employee information, you can call it Employee Information. In the **Description** field, you can type: Search employee names, addresses, and serial numbers.
4. Optional: Select the **Filter Fed Entity** to filter the federated entities displayed in the list. Filtering the choices might save you time by limiting the retrieval and display of these objects. The Filter Objects Options window displays, from which you can select your filtering preferences.
5. Click **Next** to proceed on to the next step, or, you can click a specific tab.

Defining the search criteria with the wizard

Define the parameters and defaults of your search template. By default, the order that you create your criteria is the same order that they display on the search template. You can change the criteria order in the search template and in the search results display by modifying the criteria settings on the Default Search Settings page of the wizard. You can return to this step at any time to define and modify the search criteria.

To define the search criteria, complete the following steps:

1. Select a criterion name. The default criterion names are the federated attributes that belong to the federated entity that you associated with the search template. If you want to create a name other than the defaults listed, type the name in the **Search criterion name** field. The search template that you create maps the search criteria to the federated attributes. When users enter the values for the search criteria, the search engine searches the values of the federated attributes.
2. Select a search type. **Attribute** is selected as a default. **Document** is active only when the federated entity has a federated text index associated with it.
3. Select a federated attribute. The federated attribute that you select links directly to the criterion name that you defined. You can select only a federated attribute that is associated with the federated entity that you selected on the previous page. The wizard completes the **Federated entity** field by using the name that you provided.
4. Select an operator. Only those operators that a content server can recognize appear in the list. If you select **in** or **not in** as your default operator, you must enter a value. If you select **between** or **not between** as your operators, you must enter delimiting values.
5. Click **Save the Current Criterion** to save your changes. Click **Create Another Search Criterion** to clear the fields and create another search criterion. .
6. Click **Next** to proceed on to the next step, or, you can click a specific tab.

Defining criteria settings with the wizard

You use Default Search Settings page of the wizard to design the characteristics and appearance of the search template and search results display for your users. The criteria settings control how the search template looks to the user of the client application. You do not have to set up each search criterion, however, if you do not order the criteria, the search results display in the order that you created them in the search template.

To set the results display settings, complete the following steps:

1. Select a search criterion from the **Search criteria order** list.
2. Use **Move Up** and **Move Down** to decide the order that you want the search template to display the search criteria.
3. Select a search criterion from the **Column order** list.
4. Use **Move Up** and **Move Down** to decide how you want returned search results displayed.
5. Enter a name of the column for the search criterion that you selected. For example, if you selected a criterion called Employee Number, but want to the search results column to have another name, you can rename it in the **Column heading** field as Serial Number. If you do not create an alternate name for the search results column, the column name uses the criterion name.
6. Enter the amount of character spaces that you want to allow for displaying the criterion results. By default, each criterion uses the same amount of space in the display table. For example, if you have four criteria, the default width for each criteria is 25% of the total display width.
7. Click **Next** to proceed on to the next step, or, you can click a specific tab.

Defining the default search settings with the wizard

You use the Default Search Settings page of the wizard to design the characteristics and appearance of the search template and search results display for your users.

To define the default search settings, you need to decide how to proceed with the search if a server is not responding to search queries, set the default wildcard character, and designate a folder where a user saves search results.

To set default search settings, complete the following steps:

1. Choose one of the following options to manage a search query:

Always run search

To run a search query until it gets results.

Prompt to run search

To ask users to continue the query if it fails. The search query prompts users if they want to continue each time it fails to retrieve results.

Never run search

To terminated the search after one failed attempt.

2. Choose a character that represents a wildcard character in the search template. You can have a different wildcard character for each search template that you create. You might use this option if you expect certain users to recognize a specific wildcard character.
3. Choose a folder to save search results. Federated folders allow users to persistently store their search results in the IBM Content Manager federated datastore.
4. Select **Search using all criteria (AND)** when you want a default search to contain all values of your search criteria, resulting in a much narrower list of search results, or for a broader retrieval, select **Search using any criteria (OR)**. **Search using all criteria (AND)** is the default.
5. Click **Next** to proceed on to the next step, or, you can click a specific tab.

Assigning access privileges with the wizard

In addition to defining where to look (with federated entities), what to look for (search criteria), and how to display results (settings), you must also give the users of the search template access privileges to use the search template on their client application.

Assigning access privileges to a user for a search template does not grant that user access to the content servers mapped to the template. Users must meet the security requirements for each individual content server. You must use access control lists and user management to make sure users have the proper privileges before assigning them access to a search template. You can find specific users and user groups by using the search capability in this page and give users access to use this search template. Users who are not authorized to view certain search criteria, like someone's salary, should not be given access to a search template that includes that criteria.

When you use the feature in the Search Template wizard to search for users or user groups, IBM Content Manager returns only users who have appropriate access to the requested content servers.

To assign privileges, complete the following steps:

1. Use the search capability to find those users to whom you want to give access for this search template. You can give access to individual users and user groups when you select **Users** or **Groups**. You can enter partial names in for your search, up to 256 alphanumeric characters.
2. Select one or more users or user groups from the list. Use the search field below the list to search within the list for specific users.

- If the user or user groups that you want do not display in the list, try conducting a broader search. If they still do not appear, they might not be defined to the system administration client.
 - To select more than one user, press the Ctrl key on the keyboard while clicking the names.
3. Click **Add** to add the selected users, or click **Add All** to move all users into the **Selected users and groups** list.
 - If you want to remove users, select the users and click **Remove**.
 - If you want to remove all users from the **Selected users and groups** list, click **Remove All**.
 4. Click **Next** to proceed on to the next step, or, you can click a specific tab.

Modifying an existing search template with the wizard

You can modify any aspect of a search template. To save your changes, you must click **Finish** in the wizard.

To change a search template, go to any one of the following specific steps where you want to change the settings:

- “Defining a search template with the wizard” on page 92
- “Defining the search criteria with the wizard” on page 92
- “Defining the default search settings with the wizard” on page 93
- “Defining criteria settings with the wizard” on page 93
- “Assigning access privileges with the wizard” on page 94

Important: If you use the eClient, you must restart the eClient for the search template changes to take effect. Users who are connected to the eClient might need to log out and log back in.

Creating a search template manually

Use the New Search Template window to create a search template for users to search for information across multiple content servers.

Prerequisite: You must create at least one federated entity before you can create a search template.

Important: Display values are not supported by the federated connector and IBM Information Integrator for Content system administration client. Therefore, the **Display Values** button is always disabled in the Search Template window in the IBM Information Integrator for Content system administration client.

To create a search template, complete the following steps:

1. In the Administration window, right-click **Search Template** and click **New > Nonwizard**. The New Search Template window opens.
2. Enter a name for the search template in the **Name** field.
3. Optional: Enter a description of the search template in the **Description** field.
4. Identify the users and user groups who can access this search template by selecting and adding them from the **Available groups/users** list to the **Selected groups/users** list.
5. Optional: Click the **Filter Groups/Users** button to filter the users and groups that are displayed in the list. Filtering the choices might save you time by

limiting the retrieval and display of these objects. The Filter Objects Options window displays, from which you can select your filtering preferences.

If you have previously chosen to filter users and groups, the **Available groups/users** list might be empty. You can change your filter preferences by clicking **Filter Groups/Users**.

6. Select a federated entity from the **Federated entity** list.
A federated entity can be associated with multiple text indexes. To see only the associated text indexes, click **Show associated only**.
7. Optional: Click the **Filter Fed Entity** button to filter the federated entities that are displayed in the list. Filtering the choices may save you time by limiting the retrieval and display of these objects. The Filter Objects Options window displays, from which you can select your filtering preferences.
If you have previously chosen to filter users and groups, the **Available groups/users** list may be empty. You can change your filter preferences by clicking **Filter Groups/Users**.
8. Click **Add** to open the New Search Criteria window where you can define the search criteria.
 - a. Click **Search on all criteria (AND)** for search results that satisfy all of the specified criteria. Click **Search on any criteria (OR)** for search results that satisfy any of the specified criteria.
 - b. Click **Default Settings** to open the Default Settings window where you can further define the settings of the search template.
 - c. Click **Display Results** to open the Display Results window where you can specify the column under which to display the search results, the column position, width, and display order. **Display Results** is enabled only for parametric searches
9. Click **OK** to save the template and close the window.
 - "Creating search criteria"
 - "Defining default values" on page 97
 - "Defining default settings" on page 97
 - "Defining display results" on page 98
 - "Viewing the search template" on page 98
 - "Viewing or modifying an existing search template" on page 99
 - "Copying a search template" on page 99

Creating search criteria

You can create two types of search criteria for parametric search or text search.

- To create search criteria, complete the following steps:
 1. Click **Add** in the New Search Template window. The New Search Criteria window opens.
 2. Enter a name for the search criteria in the **Name** field.
 3. Click **Parametric**.
 4. Select a federated attribute from the **Federated attribute** list.
 5. Select a default operator from the **Default operator** list. A default operator is not required for the display-only criteria.
 6. Optional: Enter a default value for the search input. To define default values for the default operators **between**, **not between**, **in**, or **not in**, click **Default value** to open the Default Value window.

7. If required, select an operator from the **Available valid operators** list in addition to the default operator. If you want to select more than one operator, press Ctrl key on the keyboard when clicking the items in the list.
 8. Click **Add** to add the selected operators to the **Selected valid operators** list.
 9. Optional: Click **Display in the results only**, if you want the user to view the results, but not to search on this criteria.
 10. Click **OK** to save the search criteria and close the window.
- To create text search criteria, complete the following steps:
 1. Click **Add** in the New Search Template window. The New Search Criteria window opens.
 2. Enter a name for the search criteria in the **Name** field.
 3. Click **Text**.
 4. Enter the default text to be searched for in the **Default search string** field.
 5. Click **OK** to add the search criteria to the search template and close the window.

Defining default values

Use the Default Values window to define the default values to use in the search template.

Requirement: You must define default values if you selected any of the following operators from the **Default operator** list in the Template Criteria window:

- in
 - not in
 - between
 - not between
- To define a default value for the default operator **in** or **not in**, complete the following steps:
 1. Click **Default Value** in the Template Criteria window. The Default Values window opens.
 2. In the **Value** field, type a default value and click **Add** to add the default value to the **Default values** list.
If you want to remove the default values, select the default values in the **Default values** list and click **Remove**. You can also remove all default values by clicking **Remove All**.
 3. Click **OK** to save the default values and close the window.
 - To define default values for the default operator **between** or **not between**, complete the following steps:
 1. Click **Default Value** in the Template Criteria window. The Default Values window opens.
 2. In the blank fields, type the default values.
 3. Click **OK** to save the default values and close the window.

Defining default settings

Use the Default Settings window to specify a default wildcard character and to indicate how to conduct searches.

To define default settings, complete the following steps:

1. Click **Default settings** in the New Search Template window. The Default Settings window opens.

2. Select any of the following default settings. These settings are used when the server is not available.

Always run search

Runs the search even if one server is not available.

Prompt to run search

Prompts the user to determine whether to continue the search if one server is not available.

Never run search

Stops the search for all servers if one server is not available.

3. In the **Default folder name** list, select a default location for the search results.
4. In the **Default wild card symbol** field, type a wildcard character for the parametric search.
5. Click **OK** to save default settings and close the window.

Defining display results

Use the Display Results window to specify the names for the columns where the search results are displayed. You also specify column position, width, and order.

To define the display results:

1. Click **Display Results** in the New Search Template window. The Display Results window opens.
2. Select a search criteria name from the **Template criteria** list.
3. In the **Display name** field, type a name for the column under which the results for the selected criteria display.
4. In the **Display position** field, specify the column position, for example 1 for the first column. If you specify 0, the results do not display.
5. In the **Display width** field, specify the width of the column.
6. In the **Criteria order** field, specify the order to display this column in the results table in the client application.
7. Click **OK** to save the display results.

Viewing the search template

Use the Search Template Viewer window to view the content of the search templates that you have created.

To view the search template:

1. Click **Tools > Search Template Viewer** from the menu bar. The Search Template Viewer window opens.
2. You can view the search template different ways:
 - To view by associated mapping, click **View > View By > Associated Mappings**.
 - To view by search template, click **View > View By > Search Template**. This view displays the search template name, template description, criteria name, search type, default operator, default value, valid operators, and default search string.
 - To view by display results, click **View > View By > Display Results**. This view displays the search template name, template description, criteria name, search type, federated entity, federated attribute, and federated text indexes.
3. Click **OK** to close the Search Template Viewer window.

Viewing or modifying an existing search template

You must regularly evaluate the quality of your search templates. You might need to change aspects of the existing search templates, or even re-create them.

To view or modify an existing search template, complete the following steps:

1. Click **Search Templates** in the tree view in the administration window to display the search templates in the right pane.
2. Right-click a search template and select **Properties**. The Search Template Properties window opens where you can view or modify all properties except for the name.
3. If you have modified properties, click **OK** to save the search template and close the window.

Important: After you change the search template, changes take place immediately. An exception to this is the eClient. If you use the eClient, you must restart the eClient for the search template changes to take effect. Users who are connected to the eClient might need to log out and log back in.

“Viewing or modifying existing search criteria”

Viewing or modifying existing search criteria:

You can view or modify search criteria for parametric search, text search, or parametric display.

To view or modify search criteria, complete the following steps:

1. Select search criteria from the **Search criteria** list in the New Search Template window or the Search Template Properties window.
2. Click **Modify**. The Template Criteria window opens where you can view or modify the properties in the window. You can modify all of the properties except the name, the federated entity, and the federated text index.
3. If you modified properties, click **OK** to save the federated entity and close the window.

Copying a search template

You might want to copy existing search templates if the existing search templates share similar properties to ones that you want to create.

To see whether an existing search template has the properties that you want to create a search template, you can view the current properties by right-clicking an existing search template and selecting **Properties**.

To copy a search template, complete the following steps:

1. Click **Search Templates** in the tree view in the Administration window to display the search templates in the right pane.
2. Right-click a search template and select **Copy**. The Copy Search Template window opens.
3. Enter a new name for the search template in the **Name** field.
4. Modify the properties as appropriate.
5. Click **OK** to save the new search template and close the window.

Deleting definitions

You can delete user, user group, server, federated entity, federated text index, or search template definitions.

Attention: If you delete a server definition, the native inventory for that server is also deleted, as are any federated mappings to native attributes on that server. This could invalidate a federated entity or any search template using that federated entity. Before you delete a server, look at your federated entities and search templates. If the server that you plan to delete is listed in an entity or template, modify the entity or template as required.

When you delete a federated entity, any search criteria referencing its federated attributes are also deleted. Deleting a federated entity could invalidate the search template. Similarly, when you delete a text search index, a search template might be invalidated.

To delete a definition, complete the following steps:

1. Click the folder from the tree view in the administration window to display the defined objects in the right pane.
2. Right-click the defined object and click **Delete**. A confirmation message window opens.
3. Click **Yes** to delete. Click **No** to cancel the action.

Assigning applications for view and launch of native data

You can choose which applications open specific types of documents by modifying or creating MIME definitions.

When adding server MIME types, verify that the document type you are adding is a MIME type created for that file. For more information, see <http://www.iana.org/assignments/media-types>.

Note that OnDemand content servers map file extensions rather than content class numeric values to MIME type streams.

To add values to the `cmbcc2mime.ini` file, complete the following steps:

1. Open `cmbcc2mime.ini` in a text editor.
2. Use the following format for user-defined values.
 - Content class starts at 4096
 - The equal sign (=) follows the content class value
 - MIME type should follow the equal sign.

To add a MIME type that is not standard for a content class, follow these steps:

- a. A MIME type is composed of a type and a subtype. Valid types are application, text, image, model, message, audio, and video.
- b. A slash (/) follows the type.
- c. To create the subtype, the token (x-) must precede the token used for that document.

```
x-mydocumentclass (4096=application/x-mydocumentclass)
```

MIME types

IBM Content Manager provides viewer support for some document types. If you define a document type to the server, you can open documents within their native

applications. For example, if you are storing Lotus® Word Pro® documents in your Content Manager OnDemand server, you can set IBM Content Manager to open files that have a .lwp extension in Lotus Word Pro, instead of opening the document in the client document viewer.

To define a document type, modify the cmbcc2mime.ini file. The file contains instructions for how to develop custom MIME definitions. The file translates content classes to a MIME type stream, so a client can read content from content servers.

Important: When opening an application based on MIME type, only the base object is displayed. Any markup that was made to the document is not displayed. If the document has multiple parts, only the first part is displayed. The MIME type in both files must match.

Adding a MIME type editor

The system administration client contains more than 10 predefined type editors. If IBM Information Integrator for Content does not list the MIME type editor that you want, complete the following steps:

1. Click **Tools > MIME Type Editor**.
2. Click **Add**.
3. Select a content server from the **Content Server** list. Depending on the content server that you select, one of the three corresponding fields activates: **Content Class**, **File Extension**, **RDB Column**. For example, when you choose IBM Content Manager as your content server, you must type a value for the editor associated with that content class in the **Content Class** field.
4. Enter the file type in the **MIME Type** field.
5. Click **OK** to save the MIME type editor and close the window. Click **Apply** to save and keep the window open to create another MIME type editor.

Adding a MIME type association

Use the MIME Type to Application Association Editor to view documents. To set up an association, complete the following steps:

1. Click **Tools > MIME To Appl. Editor**.
2. Click **Add**.
3. Choose a document type from the list provided in the **MIME Type** field.
4. In the **Application** field corresponding to the file type that you indicated in the **MIME Type** field, type the fully qualified path of the application. Make sure the application path is in the system path. For Windows servers, the application path is (%PATH%). For UNIX servers, the system path is (\$PATH).
5. Optional: Include any application options in the **Options** field. For example, for Netscape Navigator, you can type -browser.
6. Optional: In the **File Extension** field, type the file extension associated with the application that is specified in the **Application** field.
7. Decide whether you want the document contents returned from the content server as an argument in the **Use As Argument** field.
8. Click **OK** to save the MIME type association and close the window. Click **Apply** to save and keep the window open to create another MIME type association.

Getting started with content management administration

The following topics provide an overview of administration tasks for IBM Content Manager and IBM Information Integrator for Content and when to perform them. In the information center, the full set of tasks also displays in the navigation pane.

- “Getting started with IBM Content Manager administration”
- “Getting started with IBM Information Integrator for Content administration” on page 105

Related concepts

“System administration client” on page 106

Related reference

“Product names” on page 107

“Supported document formats” on page 108

Getting started with IBM Content Manager administration

The *First Steps* sample data and associated information provides an introduction to the system.

Table 12 summarizes and links to the high-level tasks for administering an IBM Content Manager system.

The system administration client provides the tools that you need to set up and manage your system. You perform some configuration tasks outside of the system administration client.

Table 12. Administration overview

Administration supertasks	What you can do	When to perform
Logging on to the system administration client	Log on to the system administration client, change your password, or, from within the client, change the server or product that you are administering.	Perform routinely.
Connecting the system administration client to the databases	Connect the system administration client to one or more local or remote library server databases in preparation for completing administration tasks.	Perform once after you install the product and have defined at least one library server.
Configuring a library server for IBM Content Manager	Configure a library server and connect the system administration client.	Perform once after you install the product and have defined at least one library server.
Defining and configuring resource managers in IBM Content Manager	Identify the resource manager to the library server. If it has not been configured already, configure Secure Sockets Layer (SSL) for the resource manager. Configure purging cycles, staging cycles, migration, and replication of resource manager objects.	Perform when you add a resource manager to your system. Perform some of these tasks when you want to view, change, copy, or delete your configuration.

Table 12. Administration overview (continued)

Administration supertasks	What you can do	When to perform
Modeling data in IBM Content Manager	Analyze your business data and model it with IBM Content Manager constructs, including attributes, item types, and links. If you plan to use the provided client applications (Client for Windows or eClient), you must use the provided document model to model your data.	Fully perform once before you put your system into production. Perform some subtasks routinely (but carefully) as your business environment changes.
Managing user access	Manage IBM Content Manager users (including IDs, groups, privileges, and data access control) and work with administrative domains.	Perform routinely as your users and business environment changes.
Managing servers in IBM Content Manager	Start and stop the application server. Optimize library server and resource manager databases. Synchronize and analyze discrepancies between servers. Validate server activity. Troubleshoot using log and trace utilities.	Perform routinely.
Managing object storage in IBM Content Manager	Create storage classes, device managers, storage systems, storage groups, and collections. Configure environment variables for resource manager utilities. Migrate, replicate, stage, and purge objects.	Perform routinely.
Managing document routing with IBM Content Manager	Analyze your environment and model your business processes in IBM Content Manager to automatically route work through a workflow process.	Optional: Perform when you want to model or automate business processes in IBM Content Manager.
Troubleshooting system administration	Fix common problems that occur during administration.	Perform when necessary.

Related concepts

“Library server” on page 5

Launching *First Steps* for IBM Content Manager

You can verify the product installation and learn basic product concepts by using the *First Steps* program.

First Steps documentation is with the *First Steps* program, a set of sample data that launches in the system administration client so that you can verify installation and learn basic concepts. To review the documentation, you must start the program.

For complete instructions on preparing and starting *First Steps*, see *Planning and Installing Your Content Management System*.

1. Start *First Steps* from the Windows or Linux workstation where you installed the system administration client.

Windows	Click Start > Programs > IBM Content Manager Enterprise Edition > First Steps .
---------	---

UNIX	Change to the <i>IBMCMROOT/firststeps</i> directory and enter: ./cm_run_firststeps.sh
------	--

The *First Steps* launchpad opens.

2. Click **First Steps Information** to open the *First Steps* documentation, which introduces basic concepts and constructs in terms of the sample data.
3. To work with the sample data, log in to the system administration client. Assuming that the default values were accepted when *First Steps* was configured during installation, you need the following values to log in:

Library server database name

icmnlbdb

Resource manager database name

rmdb

User ID

icmadmin

Password

password

Related reference

"Finding IBMCMROOT" on page 571

Getting started with IBM Information Integrator for Content administration

Table 13 summarizes and links to the high-level tasks for administering an IBM Information Integrator for Content system.

The system administration client provides the tools that you need to set up and manage your system. You perform some configuration tasks outside of the system administration client.

Table 13. Administration overview

Administration supertasks	What you can do	When to perform
Logging on to the system administration client	Log on to the system administration client, change your password, or, from within the client, change the server or product that you are administering.	Perform routinely.
Connecting the system administration client to the databases	Connect the system administration client to a local or remote administration database in preparation for completing administration tasks.	Perform once after you install the product.
Connecting content servers to IBM Content Manager	Define and configure content servers.	Perform once after you install the product and whenever you add a new content server.
Developing federated searches with IBM Content Manager	Run server inventories; map native and federated entities, and create federated searches.	Fully perform before you put your system into production. Perform some subtasks routinely to ensure that you have a current inventory and when you want to create additional searches.

Table 13. Administration overview (continued)

Administration supertasks	What you can do	When to perform
Managing user access	Manage IBM Content Manager users (including IDs, groups, privileges, and data access control) and create administrative domains.	Perform routinely as your users and business environment changes.
Managing advanced workflow with IBM Content Manager	Analyze your environment and model your business processes in IBM Content Manager to automatically route work through a workflow.	Optional: Perform when you want to model or automate business processes in IBM Content Manager.
Troubleshooting system administration	Fix common problems that occur during administration.	Perform when necessary.

System administration client

You can use the system administration client for most of your administration tasks (a few configuration tasks are accomplished with separate utilities).

If you install both IBM Content Manager and IBM Information Integrator for Content, you can access both products from the same system administration client. You can switch products without logging off from one and logging on to another, though you are prompted for a user ID and password if they are different than those you used to log on initially. You can also switch IBM Content Manager library servers or IBM Content Manager content servers without logging off and on again.

After you log on to the system administration client, you can use the mouse or keyboard access keys to navigate within it. You can control how objects are displayed in the details pane from the **View** menu.

- Click **View > Icon View** so that objects are listed along with the graphical icons that are assigned to them. Click **View > Sort Order > Sort Ascending** to display the objects in alphabetical order.
- Click **View > List View** so that objects are listed by their names. This view is the default. Click **View > Sort Order > Sort Ascending** to display the objects in alphabetical order.
- Click **View > Detail View** so that objects are listed with additional information such as their descriptions. You can sort the objects by clicking the **Name** column heading.

Attention: If you have a large number of objects and switch to **Detail View**, some of the descriptions might not display immediately. You might also experience a short pause if you click a new tree node or click **View > Refresh** when in this view with a large number of objects.

In the system administration client window, fields that are marked with an asterisk (*) are required.

Many windows include a **Display name** field. Use this field to identify a unique and meaningful name for the element that you are creating; the content of this field is displayed to client users.

Restriction: Some Linux distributions do not support right-click mouse functionality in the right details pane of the system administration client. To perform the same functions, select an object and use the **Selected** menu.

Related concepts

“Display name”

Display name

Certain windows, like the ones for attributes, item types, and MIME types, require a name and a display name. The name that you specify in the **Name** field is an internal name that uniquely identifies an element in the library server. The value in the **Display name** field is used in the Client for Windows, eClient, and other applications because it can be a more readable and understandable value than the **Name** field.

The **Name** field has a restrictive set of rules for its values. The **Display name** field allows for longer values, spaces, and other characters. Also, in some cases, you can click **Translate** to translate the display name into your national language.

Important: Use unique display names. If you do not, you can confuse your users. For example, you might have separate attributes for given names and surnames. If you use the display name of Name for both attributes, users see two attributes called Name. Therefore, users might not know which value to enter for each attribute.

Furthermore, because the display name is often more meaningful to users than the name, the client application often relies on the display name instead of the name. Frequently, client applications list all or a subset of items that are available to the user based on the display name. Some client applications might use only the display name as a key to search through the retrieved list of items. If a client application is performing this mapping, it might not be able to handle duplicate display names.

IBM Content Manager does not prohibit you from entering duplicate display names, but not all clients support such duplication. Clients might report an error, or map all items with the same display name to the first item that contains that display name. If you duplicate a display name, the system administration client returns the following warning:

Duplicate Display Name: The display name that you specified for this item is the same as the display name for another item. This duplication might cause problems for client applications.

If you are not using one of the provided client applications (eClient or Client for Windows) and your application does not rely on unique display names, you can accept this warning and no problems will result.

Some of the item types defined in the IBM Content Manager connector API samples contain duplicate display names. If you update any of the sample item type definitions by using the system administration client, you will see the described warning, which you can ignore.

Product names

In this publication, product names are sometimes used generally when there is no difference in function or usage among all supported versions.

Table 14 identifies common general terms for product names used in this publication. For information about supported versions of operating systems and prerequisite software, see *Planning and Installing Your Content Management System*.

Table 14. Product names

Term	Applies to
IBM Content Manager	IBM Content Manager Enterprise Edition and IBM Content Manager for z/OS
Content Manager EE	IBM Content Manager Enterprise Edition
Content Manager for z/OS	IBM Content Manager for z/OS
WebSphere Business Integration Server Foundation, WebSphere Application Server, and WebSphere	IBM WebSphere Business Integration Server Foundation or IBM WebSphere Application Server
DB2, DB2 UDB, and DB2 Universal Database	IBM DB2 Universal Database

The general term "Windows" applies to all supported versions of Microsoft Windows.

The general term "UNIX" applies to AIX, Linux, and Solaris in cases where there is no difference in function or usage. The general term "Linux" applies to all supported Linux distributions on all supported platforms in cases where there is no difference in function or usage.

Windows-based systems use backslashes (\) to delimit directories in a directory path. UNIX-based systems and z/OS UNIX System Services (USS) use forward slashes (/) as delimiters. This information uses backslashes (\) to delimit directories in paths that apply to all operating systems; depending on the system that you are using, you might need to enter the directory path differently than shown.

Supported document formats

The Client for Windows and the eClient support many document formats, including word processing, spreadsheet, database, presentation, compressed, and graphics formats.

The following tables list the document formats that are supported by the Client for Windows and the eClient. If you cannot find a specific file format, you can add that file format by defining a MIME type for the file format by using the system administration client.

Table 15. General Formats

File format	Extension	Supported on eClient applet viewer?	Supported on Client for Windows?	MIME types
MO:DCA (IOCA, PTOCA)	MDA	Yes	Yes*	application/vnd.ibm.modcap
TIFF	TIF	Yes	Yes	image/tiff
JPEG	JPG	Yes	Yes	image/jpeg
GIF	GIF	Yes	Yes	image/gif
PCX	PCX	Yes	Yes	image/pcx
DCX		No		

Table 15. General Formats (continued)

File format	Extension	Supported on eClient applet viewer?	Supported on Client for Windows?	MIME types
CALS			Yes	
Windows bitmaps	BMP	Yes, Windows only	Yes	image/bmp
OS/2 bitmaps	BMP		Yes	image/bmp
ASCII text	TXT	Yes	Yes	text/plain
AFP	AFP	Yes		application/afp

Table 16. Word Processing Formats: Generic Text

File format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
ASCII text	7 and 8 bit	Yes	Yes	text/plain
ANSI text	7 and 8 bit	Yes	Yes	text/plain
HTML	Through 3.0	Yes, Windows only	Yes	text/html
Microsoft Rich Text Format	All	Yes, Windows only	Yes	text/rft

Table 17. Word Processing Formats: DOS

File format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
DEC WPS Plus (DX)	Through 4.0		Yes	
DEC WPS Plus (WPL)	Through 4.1		Yes	
DisplayWrite® 2 and 3 (TXT)	All		Yes	
DisplayWriter 4 and 5	Through Release 2.0		Yes	
Enable	3.0, 4.0, and 4.5		Yes	
First Choice	3.0		Yes	
IBM Writing Assistant	1.01		Yes	
Lotus Manuscript	2.0		Yes	
MASSI I	Through 8.0		Yes	
Microsoft Word	Through 6.0	Yes, Windows only	Yes	application/msword
Microsoft Word	2007			
Microsoft Works	Through 2.0		Yes	
MultiMate	Through 4.0		Yes	
Navy DIF	All		Yes	
Nota Bene	3.0		Yes	

Table 17. Word Processing Formats: DOS (continued)

File format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Office Writer	4.0 through 6.0		Yes	
PC-File Letter	Through 3.0		Yes	
PC-File+ Letter	Through 3.0		Yes	
PFS:Write	A, B, and C		Yes	
ProfessionalWrite	Through 2.1		Yes	
Q&A	2.0		Yes	
Samna Word	Through Samna Word IV+		Yes	
SmartWare II	1.02		Yes	
Sprint	Through 1.0		Yes	
TotalWord	1.2		Yes	
Volkswriter 3 and 4	Through 1.0		Yes	
Wang PC (IWP)	Through 2.6		Yes	
WordMARC	Through Composer Plus		Yes	
WordPerfect	Through 6.1	Yes, windows only	Yes	application/wodperfect5.1
Wordstar	Through 7.0		Yes	
Wordstar 2000	Through 3.0		Yes	
Xywrite	Through III Plus		Yes	

Table 18. Word Processing Formats: International

File Format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
JustSystems Ichitaro	5.0, 6.0, 8.0, 9.0, and 10.0		Yes	

Table 19. Word Processing Formats: Windows

File format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
AMI/AMI Professional	Through 3.1		Yes	
JustWrite	Through 3.0		Yes	
Legacy	Through 1.1		Yes	
Lotus Word Pro	96 through Millennium Edition 9.6	Yes, Windows only	Yes	application/vnd.lotus-wordpro
Microsoft Windows Works	Through 4.0		Yes	

Table 19. Word Processing Formats: Windows (continued)

File format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Microsoft Windows Write	Through 3.0		Yes	
Microsoft Word for Windows	Through 2002	Yes, Windows only	Yes	application/msword
Microsoft Wordpad	All		Yes	
Novell Perfect Works	2.0		Yes	
ProfessionalWrite Plus	1.0		Yes	
Q&A Write for Windows	3.0		Yes	
StarOffice for Windows and UNIX	5.2		Yes	
WordPerfect for Windows	Through 10	Yes, Windows only	Yes	
WordStar for Windows	1.0		Yes	

Table 20. Word Processing Formats: Macintosh

File format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
MacWrite II	1.1		Yes	
Microsoft Word	4.0 through 98		Yes	
Microsoft Works	Through 2.0		Yes	
WordPerfect	1.02 through 3.0		Yes	

Table 21. Spreadsheet formats

Format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Enable	3.0, 4.0, and 4.5		Yes	
First Choice	Through 3.0		Yes	
Framework	Through 3.0		Yes	
Lotus 1-2-3® (DOS and Windows)	Through 5.0	Yes, Windows only	Yes	application/vnd.lotus-1-2-3
Lotus 1-2-3 Charts (DOS and Windows)	Through 5.0		Yes	
Lotus 1-2-3 (OS/2)	Through 2.0		Yes	

Table 21. Spreadsheet formats (continued)

Format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Lotus 1-2-3 Charts (OS/2)	Through 2.0		Yes	
Lotus 1-2-3 for SmartSuite®	97 through Millennium Edition 9.6		Yes	
Lotus Symphony	1.0, 1.1, and 2.0		Yes	
Microsoft Excel Windows (except for workbook protected files with a password)	2.1 through 2002	Yes, Windows only	Yes	application/vnd.ms-excel
Microsoft Excel Windows (except for workbook protected files with a password)	2007	Yes Note: cell is left aligned; bi-directional languages do not display correctly	Yes Note: cell is left aligned; bi-directional languages do not display correctly	
Microsoft Excel Macintosh (except for workbook protected files with a password)	3.0 through 98		Yes	
Microsoft Excel Charts (except for workbook protected files with a password)	2.x through 7.0		Yes	
Microsoft Multiplan	4.0		Yes	
Microsoft Windows Works	Through 4.0		Yes	
MicrosoftWorks (DOS)	Through 2.0		Yes	
MicrosoftWorks (Mac)	Through 2.0		Yes	
Mosaic Twin	2.5		Yes	
Novell PerfectWorks	2.0		Yes	
Quattro Pro for DOS	Through 5.0		Yes	
Quatrtrto Pro for Windows	Through 1.0		Yes	
PFS:Professional Plan	1.0		Yes	
SuperCalc 5	4.0		Yes	
SmartWare II	1.02		Yes	

Table 21. Spreadsheet formats (continued)

Format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
VP Planner 3D	1.0		Yes	

Table 22. Database Formats

File format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Access	Through 2.0		Yes	
dBASE	Through 5.0		Yes	
DataEase	4.x		Yes	
dBXL	1.3		Yes	
Enable	3.0, 4.0, and 4.5		Yes	
First Choice	Through 3.0		Yes	
FoxBase	2.1		Yes	
Framework	3.0		Yes	
Microsoft Windows Works	Through 4.0		Yes	
Microsoft Works (DOS)	Through 2.0		Yes	
Microsoft Works (Mac)	Through 2.0		Yes	
Paradox (DOS)	Through 4.0		Yes	
Paradox (Windows)	Through 1.0		Yes	
Personal R:BASE	1.0		Yes	
R:BASE	Through 3.1		Yes	
R:BASE System V	1.0		Yes	
Reflex	2.0		Yes	
Q&A	Through 2.0		Yes	
Smartware II	1.02		Yes	

Table 23. Presentation Formats

Format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Corel/Novell Presentations	Through 10		Yes	
Harvard Graphics for DOS	2.x and 3.x		Yes	
Harvard Graphics for Windows	3		Yes	
Freelance for Windows	Through Millennium Edition 9.6	Yes, Windows only	Yes	

Table 23. Presentation Formats (continued)

Format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Freelance for OS/2	Through 2.0		Yes	
Microsoft PowerPoint for Windows	3.0 through 2002	Yes, Windows only	Yes	
Microsoft PowerPoint for Windows	2007			
Microsoft PowerPoint for Macintosh	4.0 through 98		Yes	

Table 24. Graphic Formats

Format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Adobe Photoshop (PSD)	4.0		Yes	
Adobe FrameMaker (MIF)	6.0		Yes	
Adobe Portable Document Format (PDF)	Through 5.0		Yes	
AmiDraw (SDW)			Yes	
AutoCAD Interchange (DXF)	12 through 14		Yes	
Binary Group 3 Fax	All		Yes	
Bitmap (BMP, RLE, ICO, CUR, OS/2 DIB)	Windows		Yes	
CALS Raster	Type I and Type II		Yes	
Corel Draw (CDR)	6.0-8.0		Yes	
Corel Draw (CDR with TIFF header)	2.0 through 9.0		Yes	
Computer Graphics Metafile (CGM)			Yes	
Encapsulated PostScript (EPS with TIFF header only)			Yes	
GEM Paint (IMG)			Yes	
Graphics Interchange Format (GIF)		Yes	Yes	

Table 24. Graphic Formats (continued)

Format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Hewlett Package Graphics Language (HPGL)	2.0		Yes	
JPEG (JPG)		Yes	Yes	
Kodak Flash Pix (FPX)			Yes	
Kodak Photo CD (PCD)	1.0		Yes	
Lotus PIC (PIC)			Yes	
Lotus Snapshot	All		Yes	
Macintosh (PICT1 and PICT2)	Bitmap only		Yes	
MacPaint			Yes	
Micrografx Draw (DRW)	Through 4		Yes	
Micrografx Designer (DRW)	Through 3.1		Yes	
Novell perfectWorks (DRAW)	Version 2.0		Yes	
OS/2 Bitmap (BMP)	All		Yes	
PaintShop Pro (PSP)	5.0 and 5.01		Yes	
PaintShop Pro 6 (PSP)	Win32 Only		Yes	
PC Paintbrush (PCX)		Yes	Yes	
Portable Bitmap (PBM)			Yes	
Portable Graymap (PGM)			Yes	
Portable Network Graphics (PNG)	1.0		Yes	
Portable Pixmap (PPM)			Yes	
Progressive JPEG (JPG)			Yes	
Sun Raster (SRS)			Yes	
TIFF (TIF)	Through 6	Yes	Yes	
TIFF CCITT Group 3 and 4	Through 6	Yes	Yes	
Truevision TGA (Targa)	2		Yes	
Viso (preview)	4		Yes	

Table 24. Graphic Formats (continued)

Format	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Visio	5 and 2002		Yes	
Windows Enhanced Metafile (EMF)			Yes	
Windows Metafile (WMF)			Yes	
WordPerfect Graphics (WPG/WPG2)	Through 2.0		Yes	
X-Windows Bitmap (XBM)	x10 compatible		Yes	
X-Windows Dump (XDM)	x10 compatible		Yes	
X-Windows Pixmap (XPM)	x10 compatible		Yes	

Table 25. Other Formats

Format	Extension	Version	Supported on eClient?	Supported on Client for Windows?	MIME types
Microsoft Outlook Message	MSG	Text only		Yes	
Microsoft Project		98 Text only		Yes	
vCard		2.1		Yes	

Related concepts

“MIME type” on page 193

Supported document types and conversions in Java viewer toolkit

Related tasks

“Defining a MIME type” on page 192

Logging on to the system administration client

Requirement: Superadministrators must use a user ID on the operating system that has sufficient administrative authority to log on to the system administration client. For DB2 Universal Database, that authority is DBADM authority. For Oracle, the user ID must belong to the Oracle DBA user group. This rule does not apply to subadministrators, such as user administrators.

Restriction: If single sign-on is enabled, you must log on to the operating system with a user ID that has administrative authority for the database.

To log on to the system administration client:

1. If you have not already done so, start the system administration client.
2. If you have both IBM Content Manager and IBM Information Integrator for Content installed, you must choose the server type to log in to.
3. Select the server that you want to access.
4. Type a valid user ID and password. If the **User ID** and **Password** fields are disabled, single sign-on is enabled. Your computer accesses the system administration client using the same user ID that you used to log in to your operating system. You do not have to provide a user ID and password to log on.
5. Click **OK**.

Related concepts

"Combined administration" on page 118

Related tasks

"Starting the system administration client on UNIX"

"Starting the system administration client on Windows"

"Changing your password" on page 119

Related reference

"System administration client logon fails" on page 584

Starting the system administration client on UNIX

To start the system administration client:

1. Log on to the system with a valid user ID. If you use single sign-on, you must log on to the operating system with a user ID that has administrative authority for the database.
2. If you access the system administration client from a remote server, export the display. If necessary, modify the xhost settings.
3. Open a command prompt and change to *IBMCMROOT/admin/common*.
4. Enter *./cmadmin.sh* to start the system administration client.

Related reference

"Finding IBMCMROOT" on page 571

Starting the system administration client on Windows

To start the system administration client:

1. Log on to the system with a valid user ID. If you use single sign-on, you must log on to the operating system with a user ID that has administrative authority for the database.
2. Click the following menu items to start the system administration client:

Product	Path
IBM Content Manager	Start > Programs > IBM Content Manager Enterprise Edition > System Administration Client
IBM Information Integrator for Content	Start > Programs > IBM Information Integrator for Content > Administration

If you have both IBM Content Manager and IBM Information Integrator for Content installed, you can use either version of the system administration client.

Combined administration

If you have both IBM Content Manager and IBM Information Integrator for Content installed, you can switch between them without closing the system administration client. There is a list of installed products above the navigation pane of the system administration client.

To change between IBM Content Manager and IBM Information Integrator for Content, select the product from the list. The contents of the left pane will change to reflect the configuration of the selected product.

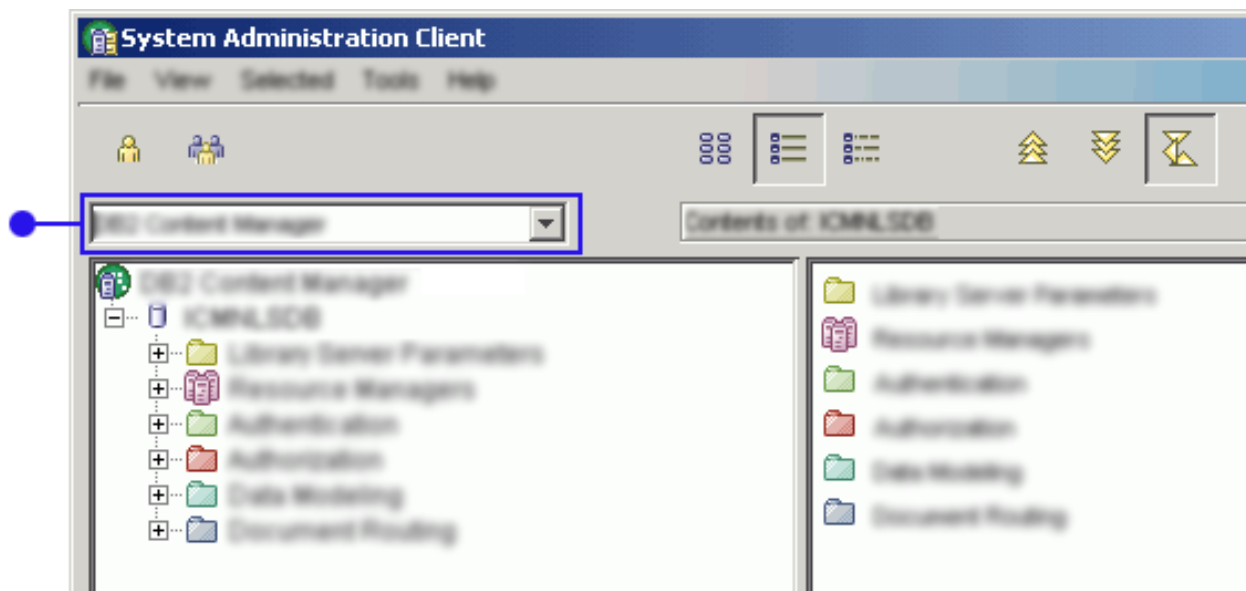


Figure 3. Product selection list

You can also administer different IBM Content Manager library servers or IBM Information Integrator for Content administration databases from the same administration session. The system administration client displays an icon for each library server and administration database it has access to. To switch to a different library server or administration database, click the icon. If the database requires a different user ID, the system prompts you to enter a user ID.

Changing your password

There are different ways to change the various passwords that are used by the IBM Content Manager system.

How you change the password for an administrator account depends on how the account was set up and what database you are using.

If you are using Oracle, an administrative user only needs to be a database user, not a system user. If a user ID is set up for the operating system and the same ID is identified for IBM Content Manager or IBM Information Integrator for Content, the ID owner must maintain both passwords.

Administrative account definition and maintenance is different for systems that use DB2 Universal Database, however.

Superadministrator accounts are always defined in the operating system, and are set up in IBM Content Manager or IBM Information Integrator for Content with the following conditions:

- The user ID must match the operating system user ID.
- The **Use System Password** option must be specified.

Subadministrator accounts can be defined like superadministrator accounts or as accounts in IBM Content Manager or IBM Information Integrator for Content, without an operating system account.

In most cases, you can use the system administration client to change the password.

Table 26. Ways to change passwords for different types of administrator accounts when using DB2 Universal Database

Administrator type	Account type	Operating system	Method to change password
Superadministrator	Operating system	AIX	Operating system or system administration client
		Linux	Operating system
		Solaris	Operating system
		Windows	Operating system or system administration client
		z/OS	Operating system

Table 26. Ways to change passwords for different types of administrator accounts when using DB2 Universal Database (continued)

Administrator type	Account type	Operating system	Method to change password
Subadministrator	Operating system	AIX	Operating system or system administration client
		Linux	Operating system
		Solaris	Operating system
		Windows	Operating system or system administration client
		z/OS	Operating system
	IBM Content Manager or IBM Information Integrator for Content	Any	System administration client

Tips: Follow your organization's policy for changing and creating passwords. In addition, consider changing the password after an upgrade or a new installation. After changing an administrative password, remember to update the password anywhere it is served, such as:

- Server definitions
- Resource manager definition
- Text search user ID in the library server configuration

To change a password in the operating system, log in to the operating system where the user account is defined and use the tool provided in that operating system for changing passwords.

To change your password from the system administration client:

1. Start the system administration client.
2. If you have both IBM Content Manager and IBM Information Integrator for Content installed, select the type of server from the **Server Type** list.
3. Select the server you want to change your password on.
4. Enter your user ID. The **Change Password** button is now enabled.
5. Click Change Password to open the Change Password window.
6. Type your current password in the **Password** field.
7. Type your new password into the **New Password** field. Your password can be 1 to 16 alphanumeric characters.
8. Type your password again for verification in the second **New Password** field.
9. Click **OK** to change your password and log in to the system administration client.

When you change an operating system account password using the system administration client, IBM Content Manager or IBM Information Integrator for Content changes the password for the operating system. Use the new password to log in to the operating system.

Related tasks

"Creating users" on page 457

"Changing the shared database connection ID and password" on page 431

Related reference

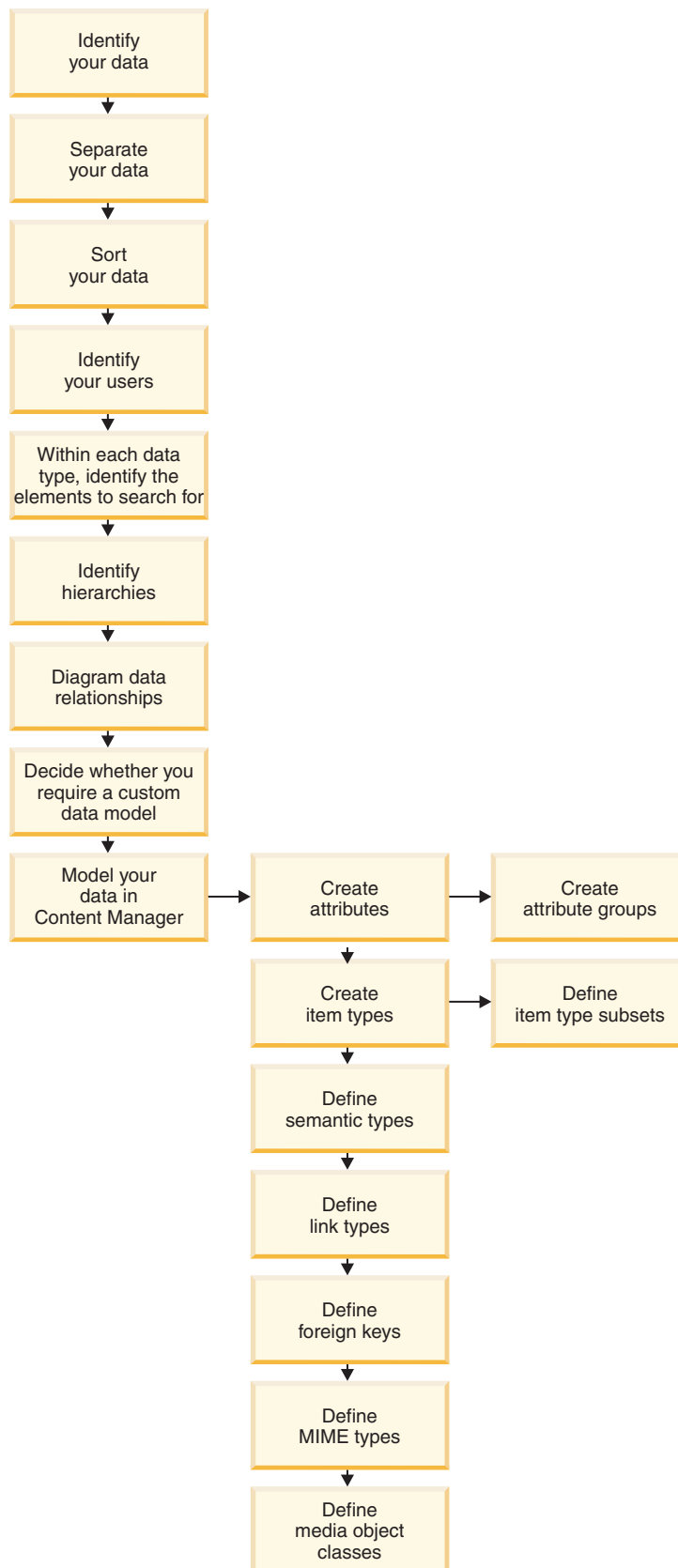
"System accounts and passwords" on page 661

Modeling your data in IBM Content Manager

To model data, you identify that data then sort it.

The following illustration shows the tasks involved in modeling your data. Each of these tasks is described in detail in the appropriate sections.

Figure 4. Common process related to modeling your data.



XYZ Insurance is a fictitious insurance company that is introduced in *Planning and Installing Your Content Management System* and is used throughout this section. Each step description ends with an example of what XYZ Insurance does to complete that step.

More information about data modeling concepts is provided in the ICM API education samples and samples readme file. If you install IBM Content Manager, see the “Getting Started” section of the ICM Samples readme file.

Windows, AIX, Solaris

README_SAMPLES_JAVA_ICM.txt located in the *IBMCMROOT/samples/java/icm* directory.

README_SAMPLES_CPP_ICM.txt located in the *IBMCMROOT/samples/cpp/icm* directory.

Linux README_SAMPLES_JAVA_ICM.txt is in: *IBMCMROOT/samples/java/icm* directory.

1. “Planning your data model”
2. “Creating an attribute” on page 146

Planning your data model

To create a data model, you start with small elements and build on them.

“Step 1: Identify your data”

“Step 2: Separate your data into operational and non-operational” on page 127

“Step 3: Sort your data into like types” on page 129

“Step 4: Identify your users and what data they need to access” on page 130

“Step 5: Within each data type, identify the elements that might be searched for” on page 132

“Step 6: Identify hierarchies and elements that might have multiple values” on page 133

“Step 7: Diagram data relationships” on page 134

“Step 8: Decide whether you require a custom data model” on page 135

“Step 9: Map your diagrammed data to an IBM Content Manager data model” on page 136

Step 1. Identify your data

To begin modeling your data in IBM Content Manager, you must first identify your data. Identifying all of the data that you want to include in the system helps you see the relationships among the data and the needs of your business. This process also exposes the requirements for your data model.

To begin integrating IBM Content Manager into your business, you might decide to begin by using it for a certain area of your business. Try to select an area that is self-contained, so that you do not need to significantly alter your model later as you add new areas.

At first, do not label or judge the data that you collect. Only identify and list it. Examples of data (either online or printed) that you might list are:

- Forms
- Documents
- Photos
- Videos

- Graphics
- Presentations
- Audio

To identify your data, you can try any or all of the following methods with a worksheet like that shown in Table 27.

Analyze your business procedures

Determine what procedures and processes your business regularly follows. Are forms, documents, or other objects required throughout these procedures and processes? Do any online forms or repositories require data entry during a procedure? Is there data, stored online or in printed format, that is an input to any step in the process?

On your worksheet, list each of these documents, forms, and data by a recognizable name. Do not worry about the order of the elements that you list. If you know who uses the elements that you list, you can indicate those names or job titles in the second column.

Identify the roles in your business

List the roles of the employees in your business and determine what each of them needs to do their jobs. You might even interview or observe representatives of different roles to see what they do and what they use to do it.

Identifying the roles, and needs of each, is especially helpful if you want to use IBM Content Manager to automatically route documents through a process. Identifying roles is also a good way to find data that should be modeled in the system but that does not fit into a recognizable business procedure or process, such as educational materials.

On your worksheet, list all of the documents, forms, and reference data that are used by each representative role in your business. List these elements by recognizable names and identify the roles who need them. If these documents, forms, or data pass through a process that you want to model in a specific order, you should indicate the order on your worksheet.

Identify your data resources

In addition to data that is used during day-to-day business, most companies have data that is used infrequently. An example of such data is materials that are used for classes or training sessions. On your worksheet, list all of this resource data that you want to include in your system.

Table 27. Worksheet 1: Data Use, columns 1 and 2

Document, form, element of data	Used by	Reserved for later steps

XYZ Insurance uses a combination of analyzing its business procedures and identifying the roles in its company to identify their data. Table 28 on page 127 shows some of the data that XYZ Insurance identifies.

Table 28. XYZ Insurance completes Worksheet 1, columns 1 and 2

Document, form, element of data	Used by	Reserved for later steps
Personal auto policy	Agent, underwriter	
Homeowners policy	Agent, underwriter	
Auto claim form	Agent, claims adjuster, underwriter, accounts payable	
Damage photos	Claims adjuster	
Police reports	Claims adjuster	
Training manual	Underwriter	
List of approved defensive driving courses	Agent	

Step 2: Separate your data into operational and non-operational

In this step, examine the list of data that you identified in the previous step, and identify which data is operational and which data is non-operational.

Operational data is the data that you need to perform business procedures and processes, for example, an insurance policy or claim form. *Non-operational data* is the information that you use for reference, research, education, and so forth, for example, materials from a training session or a videotape of a session with the company president.

Separating your data can help you make decisions about how to use IBM Content Manager effectively to model your data. The following list identifies some considerations that separating your data can help you with:

- Operational data might require workflow. You might decide to use the document routing function of IBM Content Manager or the advanced workflow of IBM Information Integrator for Content to create a routing system for operational data that follows a process, for example, a claim form that is passed from receiver to adjuster to approver to cashier.
- Operational data might require heavy client application usage. The clients that are provided by IBM Content Manager do not support all of the elements that you can use to model your data (see Table 31 on page 128). If you want to use one of the provided clients, you must model your data accordingly. You need to make an informed decision about whether to model your data using the full function of IBM Content Manager because doing so requires you to write your own client application.
- Non-operational data might not require the immediate performance expected of operational data.

Table 29 is an extension of the worksheet in Table 27 on page 126. One of the reserved columns is now labeled “Operational?” so that you can use it to indicate whether each element of data is operational or non-operational.

Table 29. Worksheet 1: Data Use, column 3

Document, form, element of data	Used by	Operational?	Reserved for next step

Table 29. Worksheet 1: Data Use, column 3 (continued)

Document, form, element of data	Used by	Operational?	Reserved for next step

In Table 30, XYZ insurance separates the data that it identified earlier into operational and non-operational.

Table 30. XYZ Insurance completes Worksheet 1, column 3

Document, form, element of data	Used by	Operational?	Reserved for next step
Personal auto policy	Agent, underwriter	Yes	
Homeowners policy	Agent, underwriter	Yes	
Auto claim form	Agent, claims adjuster, underwriter, accounts payable	Yes	
Damage photos	Claims adjuster	Yes	
Police reports	Claims adjuster	Yes	
Training manual	Underwriter	No	
List of approved defensive driving courses	Agent	No	

“Client-supported data model elements”

Client-supported data model elements

Certain data model elements might not be supported in the Client for Windows or the eClient.

Table 31 shows data model elements and whether they are supported in the clients.

Table 31. Client support for data model elements

Data model element	Supported by:	
	Client for Windows	eClient
Attribute	Yes (except for BLOB and CLOB types)	Yes (except for BLOB and CLOB types)
Attribute group	No	Yes
Root component	Yes	Yes
Child component	One level only	One level only
Item type classification: item	No	No
Item type classification: resource item	No	No
Item type classification: document	Yes	Yes

Table 31. Client support for data model elements (continued)

Data model element	Supported by:	
	Client for Windows	eClient
Item type classification: document part	Yes (client users are unaware of the presence of document parts. Creating document parts using user-defined document part types is not supported)	Yes (client users are unaware of the presence of document parts. Creating document parts using user-defined document part types is not supported)
Versions	Yes	Yes
Media object class	Yes	Yes
Item type subset (referred to as “views” in the Client for Windows)	Yes	Yes
Semantic type	Yes (semantic type support in the provided clients is transparent to the user. The clients do not provide a way for users to select from available semantic types)	Yes (semantic type support in the provided clients is transparent to the user. The clients do not provide a way for users to select from available semantic types)
MIME type	Yes	Yes
Links	Folder only	Folder only
References	No	Can be displayed
Foreign keys	No	Yes

Restriction: The use of the external table is not supported in the eClient. The eClient only handles foreign key restraints that use aIBM Content Manager item type.

Step 3: Sort your data into like types

Sorting the data into like types helps you develop a structure for your data model. After you complete this step, you will have a preliminary list of the item types that you want to create in IBM Content Manager to model your data.

Begin this step by consolidating any duplications on your worksheet.

Examine your worksheet (see Table 32 on page 130) and identify areas of commonality between elements that are listed in column 1. Use the full width of column 4 to try a combination of the following techniques for sorting the elements into like types. Sort by:

- Media type, for example, documents, videos, photographs, and so forth
- Paper forms
- Purpose
- Customer type

By using a combination of techniques, you can drill down to types that are unique and begin to uncover where unique information appears in more than one place. For example, you might sort by media type, identifying documents, videos, and photographs. You might then sort each by purpose, identifying these types of documents: insurance claim, personal auto policy, police report, fax, and so forth.

Table 32. Worksheet 1: Data Use, column 4

Document, form, element of data	Used by	Operational?	Unique types

In Table 33, XYZ Insurance sorts the data that it gathered into unique types. First XYZ Insurance sorts the data by media type, identifying scanned documents, digital photos, an online source (Microsoft Word) document, and a plain text (ASCII) list that was stored in Wordpad on an agent's desktop. The results of sorting by media type appear first in column 4 of the table.

Next, XYZ Insurance sorts by paper form, noting that the scanned documents are different enough to each require a unique type. The Damage photos and Police reports are to be associated directly with the Auto claim form. The Training manual and List of approved defensive driving courses are not related to any forms, and so are unique. However, other training manuals and lists of information might be used for reference, so these unique types should be generic enough to encompass that other data, too. The results of the second sorting pass appear second in column 4 of the table Table 33.

Table 33. XYZ Insurance completes Worksheet 1, column 4

Document, form, element of data	Used by	Operational?	Unique types
Personal auto policy	Agent, underwriter	Yes	Scanned document; Personal auto policy form
Homeowners policy	Agent, underwriter	Yes	Scanned document; Homeowners policy form
Auto claim form	Agent, claims adjuster, underwriter, accounts payable	Yes	Scanned document; Auto claim form
Damage photos	Claims adjuster	Yes	Digital photo; Detailed information for Auto claim form
Police reports	Claims adjuster	Yes	Scanned document; Detailed information for Auto claim form
Training manual	Underwriter	No	Microsoft Word document; Manual not related to a form
List of approved defensive driving courses	Agent	No	ASCII text document; Reference list not related to a form

Step 4: Identify your users and what data they need to access

As part of building your content management system, you must identify your users and provide them with appropriate access control. However, identifying your users and what they need to access at a very basic level is an important step for

building your data model. Knowing who needs what can help you determine how you use IBM Content Manager effectively.

When you build your system, you want to maximize performance. The provided clients are built to maximize performance, but they have some restrictions on the data that they display to users (Table 31 on page 128). For example, after completing this step, you might realize that, although you have many users, they need access to a small subset of the data.

Review your worksheet. If you have not already done so, use the second column to identify users (by role) for the different unique types that you identified. If you used the method of identifying business roles in Step 1 to identify your data, you have already begun to identify the users of your data. Even if you completed the second column earlier, look through it again, using the information that you entered into the fourth column.

Tip: Leave room in the second column so that you can plan your access control later.

XYZ Insurance completed the second column earlier. After reviewing the worksheet, XYZ Insurance realizes it wants to be able to print renewal policies directly from the system onto special forms, which they can send to customers. So although customers do not need direct access to the system, they are indirect users of the system in the sense that the system must provide output that is tailored for their needs.

Table 34. XYZ Insurance updates Worksheet 1, column 2

Document, form, element of data	Used by	Operational?	Unique types
Personal auto policy	Agent, underwriter, customer	Yes	Scanned document; Personal auto policy form
Homeowners policy	Agent, underwriter, customer	Yes	Scanned document; Homeowners policy form
Auto claim form	Agent, claims adjuster, underwriter, accounts payable	Yes	Scanned document; Auto claim form
Damage photos	Claims adjuster	Yes	Digital photo; Detailed information for Auto claim form
Police reports	Claims adjuster	Yes	Scanned document; Detailed information for Auto claim form
Training manual	Underwriter	No	Microsoft Word document; Manual not related to a form
List of approved defensive driving courses	Agent	No	ASCII text document; Reference list not related to a form

Related concepts

“Access control lists” on page 472

“Step 1. Identify your data” on page 125

Step 5: Within each data type, identify the elements that might be searched for

In this step, you develop the unique types that you identified. For each unique type, you identify the characteristic elements, the attributes that users of your system might use to search for items.

You must consider how you plan to use your system so that you can identify the right number of attributes to uniquely identify items of a given type.

You might decide to store few characteristic elements, just enough for users to search for and find items. For example, you might use the system to store scanned documents that users can find by entering a customer name or customer number. In such a system, users review the scanned document to see the details. Or you might use the system to store all customer information in such a way that you can print customer documents onto pre-printed forms. In this type of system, you would define many attributes, and users could search for items by entering almost anything about a customer.

In a new worksheet, like sample worksheet 2 shown in Table 35, copy the unique types that you identified on your first worksheet into the first column. Then, use the second column to identify the necessary attributes. In the third column, make any notations regarding the data type, length, and so forth of the attributes; doing this can help you later when you enter the attributes into the system.

Table 35. Worksheet 2: Retrievability, columns 1, 2, and 3

Unique types	Characteristic elements	Data type, length	Reserved for next step

Table 36 shows how XYZ Insurance identifies the characteristic elements for a couple of the unique types that they previously identified. Because XYZ Insurance wants to use the system to print policies on special forms, it must identify attributes for those forms that must conform to the special, pre-printed forms.

Table 36. XYZ Insurance completes Worksheet 2, columns 1, 2, and 3

Unique types	Characteristic elements	Data type, length	Reserved for next step
Personal auto policy form	Policy number	Alphanumeric character, 10	
	Named insured	Variable character, 128	
	Named insured address	Variable character, 512	
	Agent name and address	Variable character, 1024	
	Policy period	Date	
	Insured vehicles	N/A	
	Operators	N/A	

Table 36. XYZ Insurance completes Worksheet 2, columns 1, 2, and 3 (continued)

Unique types	Characteristic elements	Data type, length	Reserved for next step
Damage photo (detailed information for Auto claim form)	Policy number	Alphanumeric character, 10	
	Photo date	Date	
	Auto claim form number	Alphanumeric character, 8	
	Description	Variable character, 1024	
Reference list	Title	Variable character, 30	
	Description	Variable character, 1024	
	Date	Date	

Related concepts

“Attributes” on page 148

“Item type” on page 156

“Item type classification: item” on page 158

Step 6: Identify hierarchies and elements that might have multiple values

You can use IBM Content Manager to build a robust data model, for example, modeling data in a hierarchy, allowing attributes to have multiple values, or both. In this step, you examine your data from Step 5 and identify any hierarchies and any elements that might have multiple values.

Multi-valued attributes represent the simplest situation that requires you to create a child component. Unlike previous IBM Content Manager releases, with child components, you can have sets of attributes that might require multiple values, for example, an address that is made up of Street, City, State, and Postal Code. By making this set of attributes a child component, you ensure that the specified multiple values remain consistent with each other. If you have two addresses, the Street for the first address remains with its associated City, State, and Postal Code, a situation that you could not guarantee if these multi-valued attributes were separated.

By completing this step, you expand your growing data model from identified item types and their attributes to include child components.

Table 37 is an extension of worksheet 2 in the previous task. The reserved column is now labeled “Multiple values or child component” so that you can use it to identify attributes that can have multiple values or sets of attributes that should be moved into a child component. Use this column to identify attributes, or sets of attributes that might have multiple values. Also use the column to identify sets of attributes that you want to separate into a child component.

Table 37. Worksheet 2: Retrievability, column 4

Unique types	Characteristic elements	Data type, length	Multiple values or child component

In Table 38 XYZ Insurance identifies the sets of attributes that require multiple values. A personal auto policy can cover more than one vehicle and can include more than one operator (driver) who lives at the same address. XYZ Insurance wants to use child components for these sets of attributes.

Table 38. XYZ Insurance completes Worksheet 2, column 4

Unique types	Characteristic elements	Data type, length	Multiple values or child component
Personal auto policy form	Policy number	Alphanumeric character, 10	No
	Named insured	Variable character, 128	No
	Named insured address	Variable character, 512	No
	Agent name and address	Variable character, 1024	No
	Policy period	Date	No
	Insured vehicles	N/A	Yes
	Operators	N/A	Yes
Damage photo (detailed information for auto claim form)	Policy number	Alphanumeric character, 10	No
	Photo date	Date	No
	Auto claim form number	Alphanumeric character, 8	No
	Description	Variable character, 1024	No
Reference list	Title	Variable character, 30	No
	Description	Variable character, 1024	No
	Date	Date	No

Related concepts

“Attributes” on page 148

“Child component” on page 165

Step 7: Diagram data relationships

So far, the data that you gathered is a lot of words on two worksheets. You are probably aware of connections between different rows of the worksheets. By diagramming the data from the worksheets, you can get a more complete view of the model that you want to build, especially the links and references that relate different elements.

Review your completed Worksheet 2: Retrievability, to identify and diagram the connections between root and child components (and child components to grandchildren, and so forth). Also diagram relationships between item types, and indicate whether these relationships are links or references. Look especially for situations where you have data this is used repeatedly. For example, if you have some boilerplate information that is included on all your forms, you might store that in a different item type and link to it from the other item types that use that information.

If you are using the new hierarchical data model available in Version 8.4.3, then you must also identify and model the hierarchical folder relationships. You must define the connections between the hierarchical folders, beginning with a single root folder. You must also define connections between the hierarchical folders and the hierarchical item types.

Figure 17 on page 166 shows the diagram that XYZ Insurance might draw for the personal auto policy form with the Insured vehicles and Operators child components. XYZ Insurance also benefits from drawing a simple diagram showing how it wants to collect Auto claim form, Damage photo, and Police report into an Auto claim folder, and use folder links to connect the four item types.

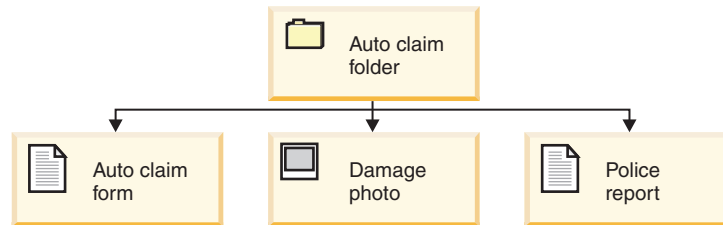


Figure 5. Simple relationship diagram

XYZ Insurance also identifies some basic customer information that it collects on most forms and does not want to repeat. XYZ Insurance separates these specific attributes into a separate type, called Customer data, which can be referenced from the various form item types.

Related concepts

“Item type” on page 156

“Root component” on page 165

“Child component” on page 165

“Link” on page 174

“Reference attribute” on page 176

Related tasks

Working with hierarchical item types

Step 8: Decide whether you require a custom data model

In this step, consider the data that you gathered and diagrammed and any other requirements for your system so that you can determine the best way to use IBM Content Manager to fit your needs.

In previous steps, particularly Step 2 and Step 4, you gathered information that can help you with this step.

IBM Content Manager provides an implementation of the data model called the document model (see “Item type classification: document” on page 160). If you decide to use the document model to model your data, you can use the provided client applications (Client for Windows and eClient) or write your own application. If you elect to design a custom data model, you must write your own application.

The provided client applications have some limitations on the data that they display to users. For example, in Step 6, did you identify a need for more than one level of child components? If so, client users will not be able to view those lower levels.

XYZ Insurance reviews the data that it gathered and diagrammed. XYZ Insurance has a large number of users (customer service personnel) who must access the basic customer and insurance data for all policies and claims. These users require high performance.

XYZ Insurance *did* identify some basic customer data that it wanted to connect with various forms using references. References are not supported by the provided clients. Furthermore, XYZ Insurance determines that it can model the rest of the data using the document model with one child component level. XYZ Insurance decides to defer the separation of basic customer data because it needs to have a solution working quickly and because of the performance needs of its users.

XYZ Insurance has, however, also identified the critical requirement that it wants to use pre-printed forms to generate renewal policies directly from IBM Content Manager. To do this effectively, XYZ Insurance decides to code a custom application.

Related concepts

“Step 2: Separate your data into operational and non-operational” on page 127

“Step 4: Identify your users and what data they need to access” on page 130

“Step 6: Identify hierarchies and elements that might have multiple values” on page 133

“Reference attribute” on page 176

“Child component” on page 165

Related reference

“Client-supported data model elements” on page 128

Step 9: Map your diagrammed data to an IBM Content Manager data model

In this step, you convert the data that you gathered and diagrammed in the previous steps into an IBM Content Manager data model.

You complete this step on paper so that when you are ready to model the data in the system, you have all the information that you need available.

You can either create a custom document model or use the provided document model.

“Creating a custom data model”

“Modeling with the default document model” on page 137

“Modeling sample data structures” on page 139

Creating a custom data model

You already gathered your data and used it to decide about how to model it in IBM Content Manager. In this step, you fit your data into a model that you can enter into IBM Content Manager, identifying the various building blocks for your elements.

Doing this step on paper before you enter the data into IBM Content Manager, helps you to enter the data more quickly and helps to avoid rework as you shuffle elements to maximize performance and reuse.

If you have enough room, you can use your two worksheets and diagrams to label your item types, resource item types, child components, links, and references. Or, you can use a new worksheet, like that shown in Table 39 on page 137 to identify this information in one location.

Table 39. Worksheet 3: Custom data model

Item types, classification: item	Item types, classification: resource item	Linked to:	Child components	Attributes	Referenced to:

See the *Application Programming Guide* and *Application Programming Reference* for specific information about writing your application.

See `SItemTypeCreationICM.java` in the `IBMCMROOT\samples\java\icm` directory for specific API information about coding an insurance application similar to the one that is described in this document. For a complete list of the samples that make up the insurance scenario, see the samples readme file: `README_SAMPLES_JAVA_ICM.txt`.

Related concepts

“Link” on page 174

“Child component” on page 165

“Reference attribute” on page 176

“Item type” on page 156

“Attributes” on page 148

“Item type classification: resource item” on page 159

 Getting started with programming content management applications

Related reference

“Finding IBMCMROOT” on page 571

Modeling with the default document model

You can model your data by using the supplied document model.

You already gathered your data and used it to decide about how to model it in IBM Content Manager. In this step, you fit your data into the supplied document model. Doing this step on paper before you begin entering the data into IBM Content Manager helps you to enter the data quickly and helps to avoid rework.

If you have enough room, you can use your two worksheets and diagrams to label your document and document part item types, your child components, and your folder links. Or you can use a new worksheet, like that shown in Table 40, to list and label this information in one place.

Table 40. Worksheet 3: Document model

Document item types	Document part item types	Child components	Attributes	Linked to:

Table 41 on page 138 shows how XYZ Insurance fits their gathered data into the document model. Note that XYZ Insurance decided to create an Auto claim folder,

which is a document item type. The Auto claim folder uses a folder link to connect with the included document part item types: Auto claim form, Damage photo, and Police report.

Table 41. XYZ Insurance completes Worksheet 3: document model

Document item types	Document part item types	Child components	Attributes	Linked or referenced to:
Personal auto policy form	Personal auto policy form base	--	See Table 37 on page 133	--
	--	Insured vehicles	<ul style="list-style-type: none"> • Year • Make • Model • Style • VIN 	--
	--	Operators	<ul style="list-style-type: none"> • Number • Name • Birth date • Sex • License number 	--
Homeowners policy form	Homeowners policy form base		<ul style="list-style-type: none"> • Policy number • Named insured • Named insured address • Agent name and address • Policy period • Covered property 	--
Auto claim folder			<ul style="list-style-type: none"> • Name • Description 	Folder link to: Auto claim form; Damage photo; Police report
	Auto claim folder notelog		...	
	Auto claim folder history		...	
Auto claim form	Auto claim form base		<ul style="list-style-type: none"> • Policy number • Named insured • Affected vehicle • Incident date • Damage description 	
Damage photo	Damage photo base		See Table 37 on page 133	--
Police report	Police report base		<ul style="list-style-type: none"> • Report number • Accident date • Officer name 	--
Training manual	Training manual base		<ul style="list-style-type: none"> • Title • Description • Author/owner • Audience 	--

Table 41. XYZ Insurance completes Worksheet 3: document model (continued)

Document item types	Document part item types	Child components	Attributes	Linked or referenced to:
Reference list	Reference list base		See Table 37 on page 133	--

- If you plan to use the provided clients, the next step is to use the worksheets to model the data.

Performance tip: When you model your data in the system administration client, you might want to create an index of the attribute values used for finding items. The index is created, in sorted order, and managed by DB2. When users search for values, matches are identified with little required I/O, which provides good response time and minimizes server CPU and I/O time. You must balance the increased performance benefit during retrieval against the relative performance cost of maintaining the index. For example, if you index every attribute in every component, you can affect the performance time for creating items.

- If you plan to write your own application:
 - See the *Application Programming Guide* and *Application Programming Reference* for specific information about writing your application.
 - For specific API information about coding an insurance application similar to the one that is described in this document, see `SItemTypeCreationICM.java`. This file is located in the `IBMCMROOT\samples\java\icm` directory. For a complete list of the samples that make up the insurance scenario, see the samples readme file: `README_SAMPLES_JAVA_ICM.txt`.
 - Use the worksheets that you created throughout this section with this book and system administration online help to model the data.

Related concepts

“Link” on page 174

“Child component” on page 165

“Attributes” on page 148

“Item type classification: document” on page 160

“Item type classification: document part” on page 160

 Getting started with programming content management applications

Related reference

“Client-supported data model elements” on page 128

Modeling sample data structures

Two scenarios describe how to model data in different situations.

The first is a very simple scenario that describes the modeling of an article for publication in a journal. The purpose is to show how child components, links, and reference attributes can be used. The second scenario is insurance-related and is meant to be more realistic and complex. An automobile insurance policy is first discussed in simple terms. Then, different methods to model the data are presented in practical terms, including a discussion of reference attributes, folders, and links.

“Scenario 1: Applying the building blocks”

“Scenario 2: Modeling automobile insurance data” on page 142

Scenario 1: Applying the building blocks:

Scenario 1 describes how the data model building blocks and concepts are applied to the modeling of an article for publication in a journal.

An article is described by attributes such as Title, Date, and Author. This can be represented as a simple item type with one component type, which is called the root component.



Figure 6. Simple item type

In a content management system, locating information can be simplified by associating a set of keywords with the document. These keywords, known as attributes, can have multiple values. Because you have multiple values, you should create a child component. In Figure 7, the third article in the Article item type has four keywords. Other articles can have different numbers of keywords.

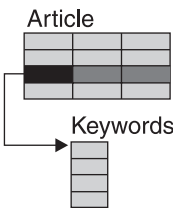


Figure 7. Item type with child component

Articles have one or more authors, as shown in Figure 8. You can define a second child component called authors such as attributes with name, company, and title.

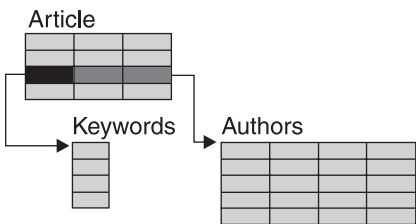


Figure 8. Item type with two child components

Although not common, consider the case where Authors might have multiple addresses. Again, you can use a child component. In Figure 9, the third article has five authors, and the third author has two addresses.

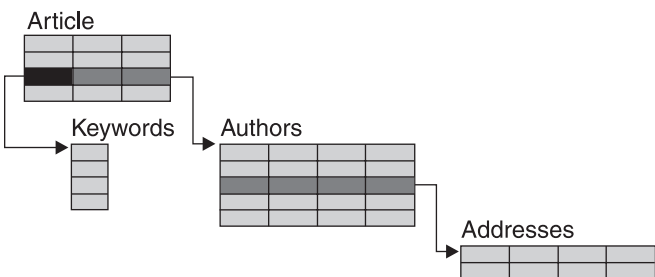


Figure 9. Item type with multiple child components

One problem is that author information is duplicated. If the same author contributed to each of the four articles, four copies of the author and address records are needed. To eliminate duplication of data, you can create a separate item type called Authors and create a relationship between Articles and Authors.

You can define three types of relationships:

- Link relationships
- Hierarchical relationships
- Reference attribute relationships

A link relationship is a loose association between two items. The link relationship contains a source item, target item, and a link type. IBM Content Manager provides link types and custom applications can define link types to model relationships not defined by the IBM Content Manager link types. The link relationship is not specific to a particular version of an item.

The link relationships are stored in the links table, separate from the source and target items. The links table contains the source ID, target ID, and link type. The Figure 10 example shows how you might use the IBM Content Manager containment link type, also known as the Contains link type, to mimic the connection of documents (articles) that are contained in a container (journal). When you use links, either the source item or target item can be deleted without affecting the other item in the relationship. Therefore, in Figure 10, if a journal is deleted, the links are also deleted. However, all of the articles remain. If a custom application requires the articles to be deleted when the journal that contains the articles is deleted, then this action must be done by the application.

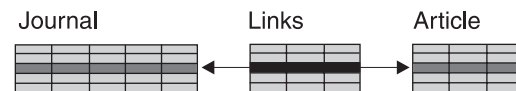


Figure 10. Example of linking

Tip: An alternative method to support a cascade delete of an item when the container item is deleted is to use reference attributes to model the relationship.

The previous example uses the containment (Contains) link type to define a basic link relationship. A different link type is used to define folder relationships. The folder contains link type, also known as DKFolder link type, models the relationship between a folder and the documents or folders that it contains. When you create a custom application, the folder relationships are handled separately from other links. You could create a hierarchy with this type of DKFolder relationship, but the creation and constraints of the hierarchy must be enforced by the application.

Beginning with IBM Content Manager Version 8.4.3, new hierarchical folder relationships are available. The hierarchical folder relationships are also modeled as links of type DKFolder. However, these relationships include constraints that are strictly enforced to model a hierarchy similar to a file system. All DKFolder relationships between item types that are marked as hierarchical are hierarchical folder relationships. Hierarchical item types are defined as either folder item types or document item types. Only the folder item types can contain hierarchical folders. All hierarchical items, folders and documents, must have a hierarchical folder as a parent. The exception is the system-defined root folder that has no parent.

The IBM Content Manager hierarchical data model includes several constraints that control the actions that can be done on hierarchical item types. For example, in a hierarchical folder relationship, a folder cannot be deleted unless it is empty. For more information about the hierarchical data model, hierarchical relationships, and constraints on hierarchical item types, see the information about working with the hierarchical item types in the programming documentation.

To create a relationship between either an item or a child component and another item, and to ensure referential integrity, you can use a reference attribute group. This type of relationship can also be used to point to a specific version of an item. A reference is stored in the source component, either root or child, and consists of the target item ID, item type, component ID, component type, and version. In Figure 11, a child component named AuthorRef is created where each row contains a reference to an author. With this approach, any number of articles, books, or other components can reference a single Author record.

Reference attributes can be displayed in the eClient.

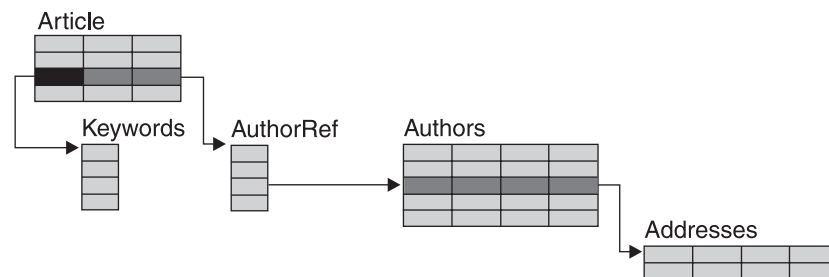


Figure 11. Example of reference attribute

Related concepts

“Attributes” on page 148

“Link” on page 174

“Child component” on page 165

“Item type” on page 156

“Reference attribute” on page 176

“Root component” on page 165

Related tasks

Working with hierarchical item types

Scenario 2: Modeling automobile insurance data:

Scenario 2 describes how to model data about automobile insurance.

An automobile insurance policy contains information about both the policy holder and the policy itself. For example, policy holder information includes the name, address, and phone number of the customer. The policy is defined by a policy number, the description of the vehicle, including the vehicle identification number (VIN) and vehicle type, deductibles for comprehensive and collision loss, driver discounts, and so forth. Some of this information has a fixed number of values, whereas other information has a variable number of values. Each automobile policy has one policy number; however, different policy holders can differ in the number and type of discounts that they receive. A sample automobile insurance

XYZ Insurance Company 442 Main Street Gladville, OH 44555										State OH Vehicle number 1MZ3872649VM Policy Number OH57839657 Policy Period Effective May 26, 2002 to Aug 15, 2002 Operators Jane Smith Joe Smith									
Insured name and address Jane Smith 321 Poplar Drive Gladville, OH 44555																			
Description of Vehicle(s)										VEH Use*									
VEH	YEAR	MAKE	MODEL	BODY TYPE	MILEAGE	IDENTIFICATION NUMBER	DYM	COMMUTE MILES											
02	02	Saturn	SL2	4D Sedan	12,540	1MZ3872649VM	8	15	15										
This location where the vehicle(s) is garaged is: (VEH 01) 321 Poplar Lane, Gladville, OH										*B=Business, W=Work, F=Farm, R=Recreation, S= School									
This policy provides ONLY the following coverages with related pricing noted.					VEH D=DED Amount Premium		VEH D=DED Amount Premium		VEH D=DED Amount Premium		VEH D=DED Amount Premium								
Part I - Liability Injury Option 1 \$ 100,000 Option 2 \$ 300,000 Option 3 \$ 25,000 Part III - Uninsured Motorist Option 1/w deductible \$100,000 Option 2/w/o deductible \$300,000 Option 3 \$500,000 Part IV - Physical Damage Coverage Comprehensive loss Collision loss Rental reimbursement Towing & Labor					1,000 22.00 1,000 128.55 500 8.45 25 5.00														
Total premium per vehicle: (For more detailed information, see the attached pages.)					752.47														
Discounts per vehicle: Anti-Theft discount \$ 9.65 Good Driver \$ 80.95 Air Bags \$ 10.45																			
1MZ3872649VM																			

You can use different methods to model this type of data. Consider the situation in which you create one item type called Policy holder, as shown in Figure 13 on page 144. This item type contains attributes such as name, address, and phone number. If this is the only item type that is defined, this model is not a good one because it does not include any content about the policy. It is merely a record containing information about customers with whom a company is doing business.

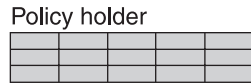


Figure 13. Policy holder item type, with no content about the policy itself

You could create one item type called Automobile policy, as shown in Figure 14. The root component might contain attributes such as policy number, those that describe the policy holder such as name, address, and phone number, and those that describe the policy such as VIN and vehicle type.

You can create a child component for this item type called Discount code. Because multiple values exist for discount codes (a customer can typically have more than one), a child component is a good place to include this type of information. Although this model does contain information about both the policy holder and policy itself, it is not the best model because of the problem of duplication of information.

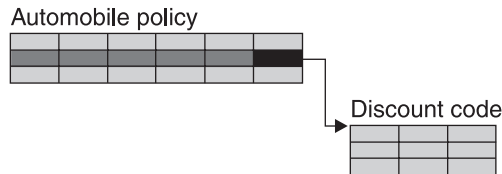


Figure 14. Automobile policy item type with child component

Consider the situation in which a customer owns more than one car. A separate policy number exists for each car that the customer owns. If three policy numbers exist for a policy holder, three copies of the policy holder's address and phone number exist.

To eliminate the problem of duplication, you can create two item types: Policy holder (with attributes such as name, address, and phone number) and Automobile policy. Instead of putting an address attribute in the Automobile policy item type, you can create a reference attribute that you use to point to the Policy holder item type, as shown in Figure 15.

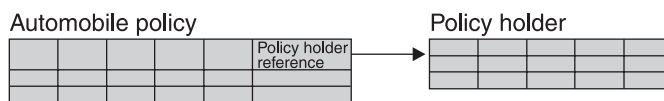


Figure 15. Automobile policy item type with reference attribute

Using the system administration client, you create a reference attribute called Policy holder in the New Reference Attribute window. On the Attributes page of the New Item Type Definition notebook for the Automobile policy item type, you can associate this reference attribute with this item type.

One potential advantage of reference attributes is referential integrity. If you select the **Restrict** delete rule on the Attributes page, you can prevent a policy holder from being deleted when a policy still exists.

Customers might have more than one type of policy. For example, they might have auto insurance, homeowners insurance, and life insurance. Another way to use child components is to create an item type called Policy holder that has a child component called Policy. The Policy child component might contain a reference

attribute that is used to point to an item in the Automobile policy, Home policy, or Life policy item type. These three item types then contain attributes that describe them. The cardinality of the child component determines how many policies a customer can have.

Another method that you can use to build a relationship between item types is linking, as shown in Figure 16. Using the system administration client, you create the Policy holder item type and classify it as a document item type. The Policy holder folders link to items from other item types, such as Automobile policy and Home policy, which contain information about these specific policies.

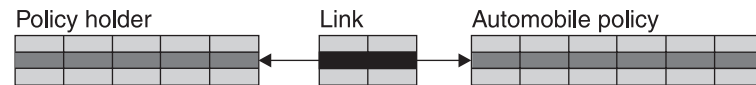


Figure 16. Linking the Policy holder folder with the Automobile policy document

The IBM Content Manager client applications allow documents or folders to be linked to folders. These items are not stored in a single place and contained within the folders as in a file system, but are linked to the folders. Documents and folders can be linked to multiple folders, whereas documents and folders typically are in one place in a file system. Using the eClient and Client for Windows, users can paste documents or add them into folders, which automatically creates the link.

Document item types generally consist of multiple document parts. With the system administration client, you can associate document parts with document item types on the Document Management page.

The IBM Content Manager client applications require that each document item type has a base part. Typically, document item types have ICMBASE (base part), ICMANNOTATION (graphical annotations that overlay the base part), and ICMNOTELOG (separate textual comments).

The main content of an item in a document item type is stored as a base part. For example, the scanned picture of a car or insurance policy is the base part of an item in the Automobile policy item type. This item might then be added to a folder in the Policy holder item type, creating a link between the Automobile policy item and the Policy holder folder.

You can automatically populate folders by setting up auto-linking. Using the system administration client, open the folder item type and, on the Auto-linking page of the New Item Type Definition notebook, add a link to the document item type using the **Folder contains** link type. The advantage of auto-linking is that the system automatically places any document that you create in the client into the folder.

You can use foreign keys for validation purposes. You use them to establish a relationship with a unique or primary key to enforce referential integrity among tables. For instance, in a Policy holder item type, you can create a unique attribute called customer number. When you create an Automobile policy item type, that item type might also have the customer number attribute. You can then define a foreign key, using the Define Foreign Key window. The foreign key points to the customer numbers in the Policy holder item type so that you cannot enter an incorrect customer number when you enter data for the automobile policy.

Related concepts

“Attributes” on page 148

“Link” on page 174

“Child component” on page 165

“Item type” on page 156

“Reference attribute” on page 176

“Root component” on page 165

“Item type classification: document” on page 160

“Item type classification: document part” on page 160

“Foreign key” on page 181

“Auto-linking” on page 188

Creating an attribute

You create an attribute to store a characteristic of an item.

An attribute stores units of data (metadata) or values that describe a certain characteristic or property (for example, first name, surname, age, city) of an item. An attribute can be used to locate that item.

To define an attribute:

1. Expand **Data Modeling** in the system administration tree.
2. Right-click **Attributes** and select **New** to open the New Attribute window.
3. In the **Name** field, type 1 to 32 characters for the attribute name. This name is the internal name and does not display in client applications.

Restriction: The name attribute can contain only uppercase and lowercase alphabetic characters, numeric characters, and the underscore (_) character. The first character in this field must be an uppercase or lowercase alphabetic character.

4. In the **Display Name** field, enter a name that displays to end users in client applications.
5. In the **Attribute type** field, select the type of information that you want the attribute to contain:
 - Click **Character** to specify that the attribute can contain alphanumeric characters that are stored at a fixed length. This is the default option and activates the **Character type** and **Character length** fields.
 - Click **Variable Character** to specify that the attribute can contain alphanumeric characters that are stored at a variable length. The client displays a variable character type attribute like a character attribute, but stores the attribute data only at the length that is needed to hold each character in the field. When you select this option, the **Character type** and **Character length** fields become active. Character length is specified in bytes. The actual maximum size and length of a variable character attribute can vary depending on your database operating system. Select a maximum size and length that is not greater than the supported level. For example, Oracle limits you to a size of about 3675. DB2 supports sizes of 28000 and higher.
 - Click **Short Integer** to specify that the attribute can contain whole numbers. The minimum is -32768 and the maximum is 32767. When you select this option, the **Integer range** field becomes active. Use the **Integer range** field to further restrict the range of the value that this attribute can contain.

- Click **Long Integer** to specify that the attribute can contain whole numbers. The minimum is -2147483648 and maximum is 2147483647. When you select this option, the **Long Integer range** field becomes active to further define the attribute.
- Click **Decimal** to specify that the attribute can contain a decimal value. When you select this option, the **Decimal length** field becomes active. There are two fields that are associated with decimal length of a decimal attribute type: **Total** and **Fixed places**. The **Total** field range is from 5 to 31 and the **Fixed places** field range is from 0 to 5. For example, if you specify 8 in the **Total** field and 2 in **Fixed places** field, then a number such as 999,999.00 can be stored.

Important: Because decimal type data can be converted to floating-point representation in other programs that work with your content management system, there might be data loss if you store extremely large numbers that approach the upper limit of the **Total** field.

- Click **Double** to specify that the attribute can contain a double precision floating point number. The maximum length is six, after which the number is rounded.
- Click **Date** to specify that the attribute can contain a date. The date is stored in the YYYY-MM-DD format.
- Click **Time** to specify that the attribute can contain time. The time is stored in the HH.MM.SS format.
- Click **Time stamp** to specify that the attribute can contain a timestamp for the application. The format of the timestamp is as follows:
YYYY-MM-DD-HH.MM.SS.NNNNNN (Year-Month-Day-Hour.Minute.Second.Microseconds).
- Click **BLOB** to specify that the attribute can contain a binary large object.
- Click **CLOB** to specify that the attribute can contain a character large object.

Restriction: On DB2, If you specify that the attribute can contain a character large object (CLOB) or a binary large object (BLOB), consider that the total amount of character or binary data that can be passed to the library server for an attribute cannot exceed 320KB. Each character attribute requires 2 additional bytes in the buffer, and the buffer used for binary data also contains control information. When developing an application that uses large attributes, consider implementing these attributes as objects on the resource manager instead.

6. Selecting **Character** or **Variable character** in the **Attribute type** group box enables the **Character type** group box.

Attention: Enforcement of the character type that you specify is done in client applications. The eClient and Client for Windows enforce character type selections, but other client applications might not.

Restriction: The client application might prevent the use of blank spaces in certain attributes.

Alphabetic

A- Z and a- z, including NLV characters.

Numeric

0-9

Alphanumeric

A-Z, a-z, and 0-9.

Extended Alphanumeric

- A-Z
- a-z
- 0-9
- a blank space
- apostrophe (')
- period (.)
- comma (,)
- colon (:)
- semicolon (;)
- question mark (?)
- quotation mark (")
- forward slash (/)
- dash (-)
- underscore (_)
- ampersand (&)
- plus sign (+)
- percent (%)
- asterisk (*)
- equals sign (=)
- greater than and less than signs (< >)
- left parentheses (()
- right parentheses ())
- vertical bar (|)
- exclamation point (!)
- dollar sign (\$)
- pound sign (#)
- caret (^)
- at sign (@)

Other Consists of any other character type.

7. Click **OK** to create the attribute.

Restriction:

- Once created, you cannot easily delete an attribute.
- You cannot change an existing attribute from numeric to extended alphanumeric. Once created, the attribute type cannot be changed.

"ICM\$NAME attribute" on page 152

Related reference

"Attribute sizing and string length considerations for non-English environments" on page 593

Attributes

An *attribute* stores units of data (metadata) or values that describe a certain characteristic or property (for example, first name, surname, age, city, and so forth) of an item. The attribute can be used in searches and queries to locate that item.

After an attribute is defined, it can be used in multiple item types. When creating attributes, you usually make them as basic as possible so that they are flexible enough to use throughout your system. You might find that you often use some of the same attributes together. For these attributes, you can create an attribute group. An *attribute group* is a set of attributes that are grouped for convenience.

You can create attributes from the main window of the system administration client or from the Attributes page in the Item Type Definition window. To create an attribute, you have to analyze the expected values for that attribute. For example, if you expect the value of an attribute to contain alphanumeric characters, then you could assign the attribute a variable character attribute type. Furthermore, you need to decide the maximum and minimum length for the variable character attribute value.

If a text search engine is installed, you enable text search in the Library Server Configuration window. Then, if you want an attribute to be text searchable, you must select the **Text searchable** check box and specify the text search parameters. For example, you might decide that the title attribute in an Article item type must be text searchable so that a librarian can find all articles with titles including the words "frog" and "green". However, you might find that making the last name attribute text searchable is not important since librarians typically know the author's last name or search with a LIKE operator and the first letter of an author's last name.

The system administration client stores the defined attributes and makes them available for selection when you create or modify item types.

System-defined and user-defined attributes

IBM Content Manager attributes can be system-defined attributes or user-defined attributes.

Table 42. Types of attributes

Attribute type	Description
system-defined	<ul style="list-style-type: none">• The attribute is created and managed by the IBM Content Manager system.• The properties are set only by the IBM Content Manager system.• The Attribute ID value is less than 1000.
user-defined	<ul style="list-style-type: none">• The attribute is created and managed by a user.• The properties are set by a user.• The Attribute ID value is greater than or equal to 1000.

Related tasks

“Viewing or modifying the library server configuration” on page 6

Defining a display name

A display name is a name that displays to users in client applications.

To define a display name:

1. Enter a meaningful name into the **Display name** field.

2. Click **Translate**. All of the available languages defined in the system are listed.
3. In the **Translated Name** column, type the translated display name for the other languages.
4. Click **OK** to save the information and close the window.

Viewing or modifying an attribute

You cannot modify most properties of an attribute that is used by an item type.

An attribute has the following properties:

- Name
- Display name
- Type
- Type-specific options that vary depending on the data type

Only the display name can be changed after the attribute is assigned to an item type.

To view or modify an attribute:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Attributes** to display all the attributes in the right pane.
3. Right-click the attribute that you want to change and click **Properties**.
4. Change the attribute information that you want to change.
5. Click **OK** to save the attribute.

Copying an attribute

You can copy an attribute by selecting an existing attribute and changing its properties.

To copy an attribute:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Attributes** to display all of the attributes in the right pane.
3. Right-click the attribute that you want to copy and click **Copy**.
4. Enter a new name for the attribute.
5. Change any attribute information that you want to change.
6. Click **OK** to save the attribute.

Deleting an attribute

You cannot delete an attribute if it is part of an attribute group or in an item type. To delete an attribute included in an attribute group or item type, you must find all of the attribute groups and items types the attribute is in and remove the attribute from them.

To delete an attribute:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Attributes** to display all of the attributes in the right pane.
3. Right-click the attribute that you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

Creating an attribute group

An attribute group is a convenient way to group one or more attributes together. For example, the "Address" attribute group might include the attributes "Street", "City", "State", and "Zip".

To create an attribute group:

1. Expand **Data Modeling** in the system administration tree.
2. Right-click **Attributes Groups** and select **New** to open the New Attribute Group window.
3. In the **Name** field, type 1 to 32 characters as the name of the attribute group.
4. In the **Display name** field, enter the name that displays to end users in client applications. Click the **Translate** button, to open the **Translate Display Name** window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
5. In the **Available attributes** list, select the attributes that you want to include in the attribute group. Click **Add** to add them to the **Group attributes** list.
6. Click **OK** to save the new attribute group definition and close the window.

Attribute group

When creating attributes, you usually make them as basic as possible so that they are flexible enough to use throughout your system. You might find that you often use some of the same attributes together. For these attributes, you can create an attribute group. An *attribute group* is a set of attributes that are grouped together for convenience.

When you add an attribute group to an item type, all attributes in the attribute group are inserted into the item type at one time. For example, instead of inserting four attributes for every item type to create an address (street, city, state, and postal code), you can create an attribute group called Address that includes those four attributes. When you create an item type, you select the attribute group Address to get the attributes: Street, City, State, and Postal Code.

You cannot set any specific properties for the attribute group; the attribute group is only for the convenience of adding several attributes at once. To set properties for the attributes, you must select them individually.

The Client for Windows and eClient applications display the attribute group name before the attribute display name.

Viewing or modifying an attribute group

You cannot change the name of an existing attribute group.

To view or modify an attribute group:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Attribute Groups** to display the list of attribute groups in the right pane.
3. Select an attribute group you want to change and click **Properties** to open the Attribute Group Properties window.
4. In the **Display name** field, type the name that displays to end users in client applications. Click the **Translate** button, to open the **Translate Display Name** window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.

5. In the **Available attributes** list, select the attributes that you want to include in the attribute group. Click **Add** to add them to the **Group attributes** list.
6. Click **OK** to save the attribute group and close the window.

Copying an attribute group

You can copy an attribute group by selecting an existing attribute group and changing its properties.

To copy an attribute group:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Attribute Groups** to display the list of attribute groups in the right pane.
3. Right-click an attribute group that you want to copy and click **Copy** to open the Copy Attribute Group window.
4. In the **Name** field, type 1 to 32 characters as a new name of the attribute group.
5. In the **Display name** field, type the name that displays to end users in client applications. Click the **Translate** button, to open the **Translate Display Name** window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
6. In the **Available attributes** list, select the attributes that you want to include in the attribute group. Click **Add** to add them to the **Group attributes** list.
7. Click **OK** to save the attribute group and close the window.

Deleting an attribute group

You cannot delete an attribute group if it is currently used in an item type.

To delete an attribute group:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Attribute Groups** to display the list of attribute groups in the right pane.
3. Right-click an attribute group you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

ICM\$NAME attribute

The ICM\$NAME attribute is a predefined user attribute that is added to a hierarchical item type.

Beginning with Version 8.4.3, you can use a new hierarchical data model to create hierarchical item types through the APIs. If the hierarchical feature is enabled on an item type, then a new attribute, ICM\$NAME, is added to that item type. Client users provide the value for the ICM\$NAME attribute, the name of the item, during item creation.

The ICM\$NAME attribute is a predefined user attribute with an AttributeID value equal to or greater than 1000. The ICM\$NAME attribute does not belong to any attribute group. It cannot be updated or deleted, and it cannot take a default value or be set to null. It cannot be added manually to a non-hierarchical item type.

After a hierarchical item type is created, you can use the ICM\$NAME attribute with some operations in the system administration client, including the following operations:

- When you are adding attributes to a hierarchical item type, the attribute is displayed in the **Selected attributes and components** list on the Attributes page. You can set the ICM\$NAME attribute to represent the item and you can use it in a text search.
- When you are adding an auto-linking rule for a hierarchical item type, the attribute is displayed in the **Current item type** attributes list on the Auto-linking page. However, you cannot link the ICM\$NAME attribute to any attribute in the **Item type to be linked to** list for the source item type. This restriction exists because the ICM\$NAME attribute exists only in a hierarchical item type and a hierarchical item type cannot be used as the source item type in an auto-linking rule.
- When you are adding a foreign key to an item type and the source or target item type is a hierarchical item type, you can use ICM\$NAME as the source or target attribute of the foreign key constraint. Select it from the **Source attributes** or **Target attributes** list, as appropriate.
- When you are creating event subscriptions for a hierarchical item type, you can use the attribute as part of the event subscription. Select it from the **Available attributes** list.
- When you are creating a database index for a hierarchical item type, you can use the attribute as part of the index by adding it to the **Assigned attributes** list.
- When you are creating an item type subset for a hierarchical item type, you can use the attribute as an attribute filter by adding it to the **Assigned attributes** list.
- When you are creating a document routing process that uses a hierarchical item type, you can use the attribute as part of the expression to define a decision point.

In other system administration client operations where this attribute cannot be used, it is hidden.

Additional information about working with the ICM\$NAME attribute is available in the programming information for IBM Content Manager.

Related tasks

Working with the ICM\$NAME attribute

Creating an item type

Create item types to define and later locate similar items.

Important: Due to caching, make sure that you click **View > Refresh** from the System Administration Client window to view the latest changes from the server. For example, if another system administrator created an item type, you can see it by clicking **Item Types** in the navigation tree and refreshing.

Important: When you create or modify an item type, ensure that all of the names, including child component names, are unique across the system. The **OK** and **Apply** buttons might not be enabled if the item type or any child component type name given already exists in the library server, or there are duplicate names in the item type being created or modified.

Restriction: Users without ItemSuperAccess privileges can only retrieve fewer than 1000 item types on Oracle because Oracle limits the maximum number of expressions in a list to 1000.

Restriction: Beginning with Version 8.4.3, a new hierarchical data model enables the creation of hierarchical item types and hierarchical folder item types to mimic the structure of a file system. However, this feature is not supported from the system administration client for Version 8.4.3. Therefore, you cannot create or view the enablement of hierarchical item types or hierarchical folder item types from the system administration client. You must use the programming information about working with hierarchical item types, including the Java or C++ API information, to work with the hierarchical data model.

To create the item type:

1. Expand **Data Modeling** in the navigation pane.
2. Right-click **Item Types** and click **New** to open the New Item Type Definition window.
3. On the Definition page, define the item type.
 - a. In the **Name** field, type 1 to 32 characters as the name of the item type. Item type names are case-sensitive and must be unique. Use names that are easy to remember and that reflect the folders and documents that are included in the item type.
 - b. In the **Display name** field, type a display name that is displayed in client applications to users. Click **Translate** to open the Translate Display Name window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
 - c. In the **New version policy** field, click **Never create**, **Always create**, or **Prompt to create** to specify whether the system always creates a new version of an item, or prompts the user decide. If you select Prompt to create, for example, the Client for Windows or eClient prompts a user to create another version of an item or update the current version of an item whenever the user edits the item's attributes.

Attention: If you specify that an attribute is unique on the Attributes page of the Item Type Definition window, then you cannot change the version policy from **Never create** to **Always create** or **Prompt to create**.

- d. If you decide to create versions, under **Maximum total versions**, specify the number of versions for the item.

When you reach the maximum total versions specified, IBM Content Manager removes the oldest version and stores the latest version.

- e. In the **Item type classification** list, specify the new item type as an item, resource item, document, or document part. By classifying the item type, you make a judgement about the purpose of the items created with this item type.

Item By classifying an item type as *item*, you determine that items of this type are self-contained, that they do not themselves describe separate stored content such as scanned documents, video, or audio.

Resource

A resource item describes and provides a connection to content that is stored on the resource manager. For example, resource items might contain pictures. If you select the resource item classification, select a media object class for the item.

Document

A document item adheres to the document model that the Client for Windows and eClient support. A document item type is not required to have associated parts.

Document part

You associate document parts with a document item type. You can associate any given document part item type with only one document item type. You associate document parts with a document in the Define Document Management Relations window, which you reach by clicking **Add** on the Document Management page of the New Item Type Definition window.

After you have made an association, you can select a specific association on the Document Management page and click **Edit** to open the Define Document Management Relations window and make a change. For example, you can associate a different access control list with a part type or modify the version policy for a part type. You can select a specific association and click **Delete** to delete the association, for example, if you specified the wrong part type. You cannot delete an association after you have stored items or you will lose parts.

- f. **Optional:** If you enabled text search from the Features page of the Library Server Configuration window, you can set up the text searches of attributes, resource items, or documents. You can enable text searching of attributes on the Attributes page.

To enable text searches of resource items and documents, select **Resource item** or **Document** from the list in the **Item type classification** field and then select **Text searchable**. You can then use the default text search parameters or click **Options** to open the Text Search Options window.

- g. If you selected **Resource item** under **Item Type Classification**, you can select a media object class that is included in the system or that you defined in the Media Object (XDO) Class window from the **Media Object (XDO) Class** field.
- h. In the **Item retention period** field, specify how long to keep an item.

Important: The **Item retention period** field does not affect how long an item is retained. If a limit is specified, the item will not be automatically deleted after the specified amount of time. The Item retention period field is for customer use only with custom applications. There is no automatic deletion from the library server.

To delete the items, you can manually select them by performing an advanced query from the Client for Windows, or you can create an application based on the samples provided in `IBMCMROOT/samples/java/icm` to perform a query for the system attribute `@EXPIRATION DATE <= current date` to select the documents that you want to delete.

- i. To automatically start an item that is created in this item type on a previously defined document routing process, select a document routing process in the **Start item on Process** field.
- j. If two types of items are started on the same process and if priority is requested in the worklist definition, you can enter an integer in the **Priority** field to indicate which of them receives higher priority. A higher number represents higher priority. There is no fixed range that you can enter.
- k. If you want to enable this item type for IBM FileNet Records Manager records management, select **Enable Records Management**. You cannot enable this item type for IBM Records Manager using this method.

Important: If you enable this item type for records management, you cannot disable it at a later time.

After you define the item type, complete its creation by completing these tasks, available from different pages of the New Item Type Definition window:

- “Selecting an access control list for the item type” on page 162
- “Adding attributes and attribute groups to the item type” on page 163
- “Specifying default storage for the item type” on page 170
- “Enabling auto-linking” on page 187
- “Defining a foreign key” on page 178
- “Logging item type events” on page 170
- “Defining document management relations” on page 171
- “Specifying user exit routines” on page 172

Click **OK** to save the new item type definition and close the window. Click **Apply** to save the information without closing the window.

Related tasks

“Defining a display name” on page 149

Working with hierarchical item types

Item type

An *item type* is a template that consists of a root component, zero or more child components, and a classification. By classifying the item type, you make a judgement about the purpose of the items created with this item type. The classifications are: item, resource item, document, and document part.

An *item* is a generic term for an instance of any item type, regardless of item type classification. For example, you might have item types called Insurance claim and Auto policy holder. Each individual claim that you create and each individual auto policy holder that you identify is generically referred to as an item.

By using the same template, items of the same type are consistently constructed, which helps you to locate them and quickly define new ones. Using IBM Content Manager, you build item types for recording a consistent set of information about the related items that you want to catalog.

In the example, the Auto policy holder item type includes a consistent set of characteristics, or attributes, for example: Policy number, Named insured, Named insured address, Vehicle make, VIN, and so forth. When you create an item of type Auto policy holder, you enter values for each of these attributes, and those values uniquely define that item.

A NOINDEX item type is available by default when you install IBM Content Manager. You should not delete this item type. You can use this item type as a model for other item types. You might also use it as a temporary placement area for items that you import or scan. You can review them and later reclassify them appropriately. The NOINDEX item type associates the following information with a new item:

- Its source, such as import or scan.
- The user ID of the operator who entered it.
- A time stamp indicating the time the item was introduced.

An ICMDRFOLDERS item type is also available by default when you install IBM Content Manager. The item type contains three attributes by default:

- A folder name, which uses variable characters

- A folder description, which uses variable characters
- A folder timestamp, which uses the timestamp attribute type

This item type is typically used by the eClient to route multiple work packages.

Beginning with Version 8.4.3, a new hierarchical data model enables you to create hierarchical item types or hierarchical folder item types through the APIs only. The system administration client does not support enablement of the hierarchical item type or hierarchical folder item type, so you cannot set or view enablement of these item types through that interface. However, after these item types are created you can view and customize some properties of hierarchical item types and hierarchical folder item types, such as the ICM\$NAME attribute, in the system administration interface.

Version policy

Some applications require an original document to be preserved and require modifications to be stored in new versions. In IBM Content Manager, you can keep multiple versions of items and objects.

Specifying version policy when creating an item type

When you create an item type, you can specify the versions for items of that type on the Definition page of the New Item Type Definition notebook. You can set one of the following version policies:

Never create

Updates a single stored item every time.

Always create

Creates a new version of the item whenever it is updated. Client users are unaware that additional versions are being created until the next time that they retrieve the item.

Prompt to create

Allows client users to decide whether to update the version they are editing or store the updates in a new version. The Client for Windows or eClient prompts a user to create another version of an item or update the current version of an item whenever the user edits the item's attributes.

The version policy that you set on the Definition page applies to attribute values. For example, if you set the version policy to allow multiple versions of items, then a user might change the value of the Surname attribute from Sanchez to Garcia and thus create a new, updated version of the item.

Restriction: If a resource item is enabled for versioning and you want to change its attributes, you can do so only by creating a copy of the resource item. You cannot update the attributes by checking in a new version of the resource item.

If you set the version policy to allow multiple versions, you can set a maximum number of versions or allow an unlimited number. If you set a maximum number, when the specified maximum is reached, the oldest version is deleted and the most recent version is saved.

If the item type that you are creating is classified as a resource item or document part, the version policy applies also to the object on the resource manager.

If the item type that you are creating is a document, you can specify supplemental version policy information for the specific document parts. You specify this

information in the Define Document Management Relations window, which you reach from the Document Management page. The version policies are independent of each other and can be enabled separately.

You can set one of the following version policies specifically for document parts:

Never create

Does not allow multiple versions of the selected document part.

Always create

Create a version of the selected document part whenever that object is edited.

Prompt to create

Allows client users to decide whether to update the version they are editing or store the updates in a new version.

The version policy for document parts supplements the version policy that you set on the Definition page. For example, on the Definition page, you might allow a maximum of three multiple versions. In the Define Document Management Relations window, you might specify Never create for the base part, but Always create for the notelog and annotation parts. In this case, one version of the base part and up to three versions each of the notelog and annotation parts can exist at any given time.

In the document model, versioning is specified at the document level and at the part level. If versioning for both the document and part are on, and if you create a new version of the part, a new version of the document is created. If parts are merely replaced (no new version of the part is created) and attributes are not changed, a new version of the document is not created.

Attention: Auto-linking is possible for document item types that are enabled for versioning. The folder item type to be linked to must not be enabled for versioning. The links for the document item type are maintained using the attributes of the current version of the item.

Converting an item type from the Never create version policy

The conversion of an existing item type from the Never create version policy to Always create or Prompt to create will be rejected if the item type has unique attributes, or if it has created a unique component index on one or more attributes. The reason is that during the conversion, IBM Content Manager checks the component tables for unique indexes that are already defined with user attributes. These indexes consist only of columns that correspond to the user attributes.

If such an index is found, the operation is rejected because item types that are enabled for versioning cannot have unique indexes on their attributes. When a new version create or update operation is attempted, a unique index causes failure because the new version will have the same value of the attributes. This problem causes a database duplicate index error.

In this case, an error message advises users to remove the unique index or indexes manually by using the system administration client or the database tool before trying the operation again.

Item type classification: item

You use item types to create items. Although some items (resource items) can describe content that is stored on the resource manager, others are self-contained.

Items are typically those things that you can describe completely with a set of attributes and are not a document or a file. Items are similar to a row in a database.

By classifying an item type as *item*, you determine that items of this type are self-contained, that they do not themselves describe separate stored content such as scanned documents, video, or audio. A common use of item classification is for item types that only have folders. The item type is a folder, and the contents of the folder are many different item types.

Examples of item types that you might classify as item:

- Customer identification data, for example, name, address, phone number
- Account identification data, for example, account holder, account number, account type
- Library catalog information for physical books, videos, CDs

In general, you classify as item those item types that you want to use to store attributes only.

Restriction: Item types that are classified as item are not supported by the provided Client for Windows or eClient.

Item type classification: resource item

Resource items describe and provide a connection to content that is stored on the resource manager.

Examples of item types that you might classify as resource item:

- Roster of videotaped seminars that users can view over the Internet or your intranet
- Auto insurance accident data, such as photos and scanned police reports
- Library catalog information for scanned, digitally stored journals

When your users find resource items, they can view or launch the referred-to content directly from that resource item.

Restriction: Item types that are classified as resource item are not supported by the provided Client for Windows or eClient.

To improve performance, the original file name of the resource item is stored in the library server as an attribute of the resource item. To take advantage of this performance improvement to retrieve the original file name, you must run the original file name transfer utility so that the original file name information for any existing resource items are moved from the resource manager to the library server.

Restriction: If a resource item is enabled for versioning and you want to change its attributes, you can do so only by creating a copy of the resource item. You cannot update the attributes by checking in a new version of the resource item.

To run the original file name transfer utility, run the following command from the command line:

Windows

```
IBMCMROOT\dbutil\icmupdrmf.bat
```

UNIX `IBMCMROOT/dbutil/icmupdrmf.sh`

Tip: The original file name of a resource item is the file name of the item before it is stored in the IBM Content Manager system.

Item type classification: document

IBM Content Manager supplies a data model implementation that you can use, called the *document model*.

The document model is similar to other document management systems and to previous releases of ImagePlus and IBM Content Manager in that it supports multipart documents with related content. For example, subsets of pages are in different parts with associated graphical annotations and notes.

Modeling your data with the supplied document model instead of creating a similar data model from scratch has the following advantages:

- You can use the client applications that IBM Content Manager provides.
- The performance of your system is better, because of the performance enhancements explicitly built into IBM Content Manager specifically for the document model implementation.
- Writing your own application is simpler, because many of the decisions you might have to make have already been made.

When you classify an item type as document, you specify that this item type adheres to the document model. Examples of item types that you might classify as document:

- A journal article
- A journal
- A folder
- An insurance policy

A document item type is not required to have associated parts, for example a folder or similar container that is metadata only. Remembering that the document model is a data model implementation, you can see that a document item type without associated parts is similar to an item type that is classified as item. Associated parts are often annotation and notelog parts.

If a document item type does have associated parts, they are managed in a parts list, which is a hidden child component of the document item type. You create the document parts first and then associate them with a document item type in the New Item Type Definition window on the Document Management page.

Requirement: Although a document item type is not required to have associated parts, a document item type must have at least one associated base part, even if it is empty, to be displayed in the eClient.

Item type classification: document part

The provided document model includes an item type classification of *document part*. After you classify item types as document part, you then associate the document parts with a document item type.

You can associate any given document part item type only once with a document item type; you cannot reuse document part item types in the same document item type.

When you associate the document parts with a document, you can select one of the five predefined document part item types:

ICMANNOTATION

Contains additions to, or commentary about, the main data; following the document metaphor, annotations include sticky notes, color highlights, stamps, and other graphical annotations in the text of a document.

These are the typical annotation parts from previous releases of IBM Content Manager. Using the Client for Windows or the eClient, your users can create graphical annotations, which are viewed on top of the file or document being displayed. Most client applications can show or hide these annotations.

ICMBASE

Contains the fundamental content of a document item type that stores any non-textual type of content, including image and audio.

Requirement: To be viewable in the eClient, all document item types must include at least one base document part.

ICMBASETEXT

Contains the fundamental content of a document item type that stores text content. If you plan to index a text part of your document, you should store the part in this part item type. Indexing a text part allows text search to be performed on the content of the part.

ICMNOTELOG

Contains a log of information entered by users. For example, indicating the reason that the insurance application was denied or instructions to the next reviewer of the document.

These are the typical notelog parts from previous releases of IBM Content Manager. Using the Client for Windows or the eClient, your users can create, view, and edit notelog parts. Notelog parts contain the user ID, timestamp, and text comments as entered by client users.

ICMBASESTREAM

Contains streamed data, such as video.

To import or scan from the Client for Windows, you must use one of the following types:

- ICMBASE for the basic part to import or scan any type of documents.
- ICMBASESTREAM to be able to import streamable documents
- ICMBASETEXT to be able to import text searchable documents.

Scanning will fail if the item type does not contain part type ICMBASE. To be sure that a user can import any type of document, part type ICMBASE must be added to the item type. If ICMBASESTREAM or ICMBASETEXT are selected, you will only be able to import documents if the MIME type is streamable or text searchable, respectively.

Examples of streamable and text searchable MIME types include:

Streamable

Basic audio, MPEG audio and video, MIDI audio, QuickTime movie, VideoCharger plugin

Text searchable

HTML, XML, Plain Text, Microsoft Word, Lotus 123, PDF, RTE, Microsoft Excel

To improve performance, the original file name of the document part is stored in the library server as an attribute of the document part. To take advantage of this performance improvement to retrieve the original file name, you must run the original file name transfer utility so that the original file name information for any existing document parts are moved from the resource manager to the library server.

To run the original file name transfer utility, run the following command from the command line:

Windows

```
IBMCMROOT\dbutil\icmupdrmf.bat
```

UNIX `IBMCMROOT/dbutil/icmupdrmf.sh`

Selecting an access control list for the item type

You can associate an item type with an ACL in the New Item Type Definition window.

To select an access control list for the item type:

1. From the New Item Type Definition window, click the **Access Control** tab.
2. Select the access control list that you want to associate with this item type. An access control list consists of users and user groups and privileges associated with each. When you associate an access control list with an item type, only the users on that list can access objects created in the system under this item type. The actions that users can perform on these objects depends on the privileges associated with them in the access control list.
3. **Optional:** To create a new association, click the **Create Access Control List** button to open the Create ACL window and create the association.
4. In the **Check ACL at** field, specify whether the access control list applies to the item type level or item level. If you specify item type level, the access control list applies to the entire item type, and the item level access control list is ignored. If you specify item level, the access control list applies to an individual item.
5. In the **For item level ACL checking, assign ACL from** field, specify the access control list to apply to the item. If you provide an access control list when an item is created, that access control list is used for actions performed on that item. The IBM Content Manager clients currently do not support users providing an access control list when creating an item.
 - If you select **Item type's ACL**, the access control list that was defined above is used. Only users on that list can access objects in that item type.
 - If you select **User's default ACL**, the access control list that was defined on the New User window is used.

In the document data model, if you select item level ACL checking, the ACL checking is applied to the item attributes, not the item parts. By default, system defined document parts, such as ICMBASE and ICMBASETEXT, use item type level ACL checking. If you require item level ACL checking for item parts, you must define your own document parts using item level ACL checking. You can then add the parts you defined to your document data model, which enables item level ACL checking for your document parts.

Related tasks

“Creating access control lists” on page 471

Adding attributes and attribute groups to the item type

An attribute stores units of data (metadata) or values that describe a certain characteristic or property (for example, first name, surname, age, city, and so forth) of an item. The attribute can be used to locate that item. The more attributes you add to an item type, the easier it will be to find a specific item under that item type.

To add attributes and attribute groups to the item type:

1. Click the **Attributes** tab.
2. Select the attributes or attribute groups that you want to add into the item type from the **Available attributes or groups** list. Click **Add** to add them to the **Selected attributes and components** list.
 - a. If you add a regular attribute, you can specify whether it is required or unique, and whether it represents the item in client applications. You can also enter the default value for the attribute. If it is an integer type, you can modify the minimum and maximum values. When you add a unique attribute, database indexes are automatically created for performance purposes. For more information, see “Automatically created database indexes” on page 199.

Tip: When you define an item type, the system administration client permits you to specify minimum and maximum values for attributes of integer types only. This range can be different from the one originally specified in the attribute definition, or for the same attribute in another item type definition.

If you specify a default value for an integer attribute, it must be within range of the minimum and maximum values you specify. However, other attribute types are not checked, and it is your responsibility to ensure that they are valid values. After you create the item type, you should test the default value by using a client to ensure that it is valid.

Attention: If you plan to create a foreign key definition by using this attribute, you must specify that it is required. You must use required attributes to create a foreign key definition.

Restriction: You can select more than one attribute to represent items. When more than one is selected, your application can concatenate the attributes (by using whatever delimiter that you want) to represent the item. However, the beans and clients do not support multiple attributes to represent items. They allow only the first attribute to be used.

- b. If you add a reference attribute, specify a delete rule. You can use a reference attribute to point to specific information that is contained in another item.
 - If you specify **Cascade**, the source component is deleted when the target component is deleted.
 - If you specify **Restrict**, you cannot delete the target because it is referenced by the source.
 - If you specify **Set null** or **No action**, when the target is deleted, the source is set to null or no action is taken.

Important: If you specified **Always create** or **Prompt to create** in the **New version policy** field on the Definition page, only the **No action** and **Restrict** delete rules for reference attributes are enabled.

- c. If the item type is a hierarchical item type, then the ICM\$NAME attribute is shown in the **Selected attributes and components** list. You can set the ICM\$NAME attribute to represent the item and can use it in a text search. The attribute is set as required and unique and you cannot change these properties.

Restriction: You cannot add the ICM\$NAME attribute to any item type from the system administration client and you cannot remove it from a hierarchical item type. Also, you cannot set a default value for this attribute.

- 3. When you add regular attributes into the item type, you can enable text searching by selecting the **Text searchable** check box and clicking **Options** to open the Text Search Options window.
- 4. Optional: Click **Add/New Child** to add a child component. A child component is an optional second or lower level of an item type. Each child component is directly associated with the level above it. If you specified **Document part** as the item type classification, you cannot add a child component.
 - a. Type the name in the **Child component name** field.
 - b. In the **Display name** field, type the name to display to end users in client applications.
 - c. Click **Translate** to open the Translate Display Name window. All of the available languages that are defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
 - d. In the **Delete rule** field, click **Restrict** to specify that the root component cannot be deleted if there is a child component and click **Cascade** to specify that when the root component is deleted, the child component is also deleted.
 - e. In the **Minimum cardinality** and **Maximum cardinality** fields, type the minimum and maximum number of entries in the child component for each item.
- 5. Optional: If you want to define default table spaces for the item type root or child components, indexes, and LOB attributes (Enterprise Edition) or default table spaces for item type root or child components (z/OS), click **Set** in the Table spaces area. Supply the custom table space names and click **OK** to save the information.

Restriction: A table space must exist in the database before you can use it as a custom table space.

“Setting default table spaces for item type components, indexes, and LOB attributes” on page 166

“Setting default table spaces for item type components for Content Manager for z/OS” on page 167

Related tasks

Working with hierarchical item types

Component

A *component* is a meaningful set of system-defined and user-defined attributes that you use to describe a type of data or some subset of it. There are two types of components, root and child. You can build item types by using one root component and zero or more child components.

In the underlying relational database, each component is represented by a table. Database indexing is available, and you define indexes at the component level.

Root component: A *root component* is the first or only level of an item type and consists of both system- and user-defined attributes. For example, a personal auto policy item type might have a root component that includes the following user-defined attributes.

Policy number	Named insured	Named insured address	Vehicle make	Vehicle model	Vehicle Identification number (VIN)	...
---------------	---------------	-----------------------	--------------	---------------	-------------------------------------	-----

This kind of item type did not exist before Version 8, so index classes that were created with earlier IBM Content Manager versions were a single level with multi-valued attributes and index class subsets. In IBM Content Manager Version 8, you can create a similar item type by creating one that has only a root component. Multi-valued attributes in IBM Content Manager Version 8 are implemented as child components. See “Child component” for more information. Index class subsets are implemented as item type subsets. See “Item type subset” on page 201 for more information.

When you work with an item type, you might change the root component to account for the child components that you plan to create. The previous example might work well for a root component with no children. However, if you planned to create children, you might create this root component:

Policy number	Named insured	Named insured address	Insured vehicles	Operators	...
---------------	---------------	-----------------------	------------------	-----------	-----

Because a customer might insure more than one vehicle, the vehicle information, such as the make, model, and vehicle identification number (VIN), might be contained in a child component. Similarly, you might create a child component to store the multiple operators (residents in a customer's home who can drive or operate the insured vehicles) that are insured under the policy.

Child component: A *child component* is the optional second or lower level of an item type. Each child component is directly associated with the level above it. Use child components for detailed information for which multiple values might exist, information that previously (in earlier Content Manager releases) might have been contained in multi-valued attributes.

For example, Figure 17 on page 166 shows the personal auto policy item type with two child components. One child component is for the vehicles that are insured under the policy. The other identifies the operators of the insured vehicles who are explicitly covered under the policy, for example, other members of the same household who can drive.

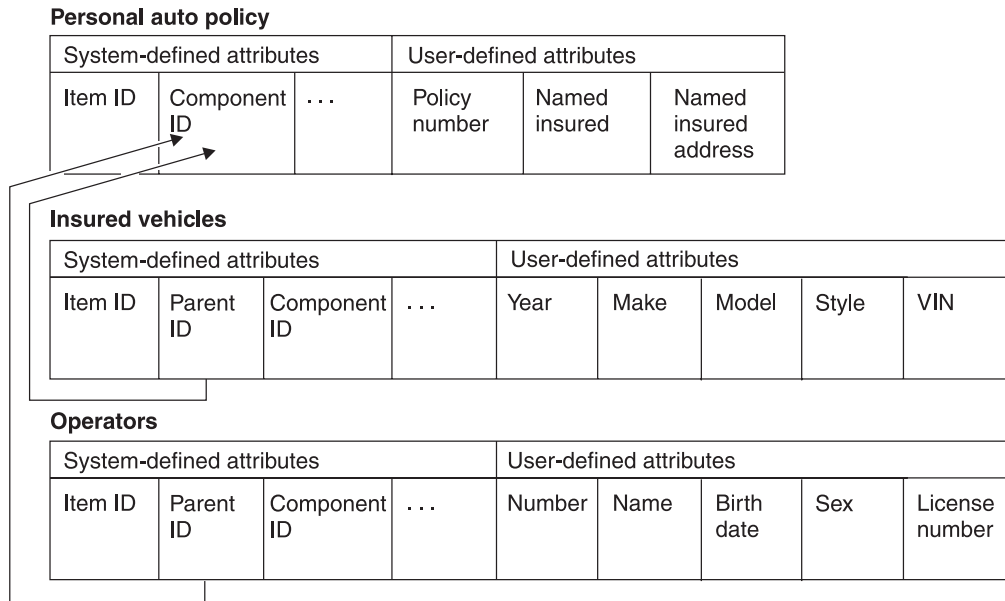


Figure 17. Item type with two child components. Parent IDs in the child components connect to the component ID in the root (or parent) component.

There is no limit to the number of component levels that you can create or to the number of children that you can include at each level. However, if you plan to use the provided Client for Windows or eClient, be aware that these clients display only one child component level.

You create child components by clicking the child component icon (the fourth icon under Select attributes and components) on the Attributes page of the New Item Type Definition notebook. After you click the child component button, the Attribute page changes so that you can set properties for the child component.

When you select a child component under **Selected attributes and components**, the fields are available for you to specify the following information:

- Name of the child component (**Child component name**).
- Name of the child component to display to client users (**Display name**).
- Whether to delete children of this child component (**Cascade**) if this child component is deleted. Note that this applies to created items that include this child component, not to the child component definition.

If you do not want to automatically delete children, click **Restrict**.

- The minimum and maximum number of rows in the database table that is created for this child component (**Minimum cardinality** and **Maximum cardinality**). For example, for the Operators and Insured vehicles child components, the minimum cardinality would be one because you cannot have an auto policy with no insured vehicles or drivers.

Although you specify a maximum cardinality, the storage space is not allocated until it is needed to store values.

Setting default table spaces for item type components, indexes, and LOB attributes

You can use the system administration client to customize your library server database by setting default table, index, and large object (LOB) table spaces for

item type root and child components, indexes, and LOB attributes. Using these customized table spaces can increase the efficiency of database management and can increase database performance.

Before you can set a default table space for an item type component, index, or LOB attribute, the table space must exist in the database.

Beginning with IBM Content Manager Version 8.4.2, you can use the system administration client to set default table spaces for new item type root and child components and indexes, including the table, index, and LOB attributes. You can also set default table spaces for new child components of item types that existed in previous versions of IBM Content Manager. For an IBM Content Manager system that uses the Oracle database, you can modify the table spaces, with some limitations on the modifications that you can perform.

Setting default table spaces for item type components, indexes, and LOB attributes is an optional step. If you do not set default table spaces for your components, indexes, and LOB attributes, then the default predefined table spaces are used for the item type root and child component tables, indexes, and LOB attributes.

To define a default table space for an item type component, index, or LOB attribute:

1. On the Attributes page of the New Item Type Definition window, click **Set** in the Table spaces area.
2. Type the name of the table space for the table in the **Table table space** field. For a DB2 database, this table space must be a database-managed space (DMS) if you supply values for the index and LOB table spaces. Also for a DB2 database, you must supply a value in this field before you can supply a value for the index or LOB table spaces. For an Oracle database, there are no restrictions on the type of table space.
3. Type the name of the table space for the index in the **Default index table space** field. For a DB2 database, this table space must be a database-managed space (DMS) and cannot be a system-managed space (SMS). For an Oracle database, there are no restrictions on the type of table space.
4. Type the name of the table space for the LOB table in the **Default large object (LOB) table space**. For a DB2 database, this table space must be a large database-managed space (DMS) and cannot be a system-managed space (SMS). For an Oracle database, there are no restrictions on the type of table space.
5. Click **OK** to save the changes and return to the Attributes page.

Related concepts

Planning custom table spaces for item type components and indexes to improve performance

Related tasks

Optimizing IBM Content Manager databases for specific requirements after IBM Content Manager installation

Creating an IBM Content Manager library server database with the Oracle DBCA template

Setting default table spaces for item type components for Content Manager for z/OS

You can customize your library server database by setting default table spaces for item type root and child components.

Before you can set a default table space for an item type component, the table space must exist in the database. Also, the OptionText value for the TABLE OptionKey value must be set to +PREDEFINED+ in the ICMST390Control table.

Beginning with Content Manager for z/OS Version 8.4.2, you can customize your library server database by setting default table table spaces for item type root and child components, in addition to using the default ICMLFQ32 table space or generating a table space for each item type or component type. The ICMST390Control table contains a new OptionText value for the TABLE OptionKey to enable you to customize the table table spaces.

By using this new function, you can use the system administration client to set default table spaces for new item type root and child components. You can also set default table spaces for new child components of item types that existed in previous versions of DB2 Content Manager.

For earlier versions of Content Manager for z/OS, you manage the table space for the table by updating the ICMST390Control table. For Version 8.4.2, you assign the table table space directly in the system administration client. To assign the table table space name in the system administration client, you must set the OptionText value to +PREDEFINED+ when the OptionKey value is set to TABLE in the ICMST390Control table.

Important: In the newer method of managing the table space for Version 8.4.2 and later, you do not need to have a row where the value of OptionKey is set to SPACE in the ICMST390Control table. If you have this row in your table, the row is ignored.

Restriction: You cannot change the index table space and the LOB attribute table space in any version of Content Manager for z/OS. The default index table space is defined by DB2 for z/OS. The default LOB attribute table space is defined by Content Manager for z/OS and is associated with the component type ID.

To define a default table space for an item type component:

1. On the Attributes page of the New Item Type Definition window, click **Set** in the Table spaces area.
2. Type the name of the table space for the table in the **Table table space** field. If the OptionText value is set to +PREDEFINED+ for the TABLE OptionKey but you do not provide a value for the default table table space, you might receive an error message immediately. However, you might not receive this error message until after you submit the JCL job. The difference in the timing of the error message depends upon how you prepare the skeleton job to create component tables and views.
3. Click **OK** to save the changes and return to the Attributes page.

You can also create a new item type by copying from an existing item type. When you do so, the table table space name from the existing item type might appear in the **Table table space** field for the new item type. However, whether the existing table table space is actually copied to the new item type depends upon the settings in the ICMST390Control table when you perform the copy action. For example:

- If your ICMST390Control table has the default setting, with OptionText set to ICMLFQ32 and the OptionKey set to TABLE, then the new item type will have the default ICMLFQ32 table space.
- If your ICMST390Control table has the OptionText set to TS+ITEMTYPEID+ or TS+COMPID+ and the OptionKey set to TABLE, then the new item type will have a

table space similar to the following example: TS01008. The new item type will not have the same table space as the existing item type.

- If your ICMST390Control table has the OptionText set to +PREDEFINED+ and the OptionKey set to TABLE, then the table space setting from the existing item type will be copied to the table space setting for the new item type.

Related concepts

Planning custom table spaces for item type components for z/OS

Related information

ICMST390Control table

Filtering objects from display in IBM Content Manager

To limit the retrieval and display of objects that have large volumes, you can filter what you want the system administration client to display.

1. From the main menu, select **Tools > Filter Object Options** to open the Filter Objects Options window.
2. Check one or more of the following boxes:
 - **User**
 - **User groups**
 - **ACL**
 - **Item Types**

By default, no object is selected.

3. Click **OK**.

If an object is checked for filtering, the next time you open a system administration window that displays that item, the Filter object window opens to enable you to define what you would like to display.

The system administration client saves the options you select and remembers them for the next session.

Filter object

After you select an object for filtering, the next time the system administration client needs to display that object, you are prompted to choose how you want to limit the display of the object. Alternately, you can right-click the object from the system administration tree and select **Filter and Explore**.

1. From the Filter *object* window, you can select one of the following choices:
 - **Show all objects**: Selecting this button displays all of the selected objects
 - **Only show objects**: Selecting this button enables you to further filter the display by choosing specific text to look for:
2. If you selected **Only show objects**, select how to filter the objects:
 - Starting with
 - Containing
 - Ending with

Specify the text to filter. For example, to display only users whose given name is Jane, select **Starting with** and enter Jane in the text field. Do not include spaces or wildcard characters.

3. Click **OK**.

The system administration client saves the options you select and remembers them for the next session. To change the filtering options, you can select **Tools > Filter Object Options** from the main menu.

Specifying default storage for the item type

You can specify default storage options for resource items. To specify default storage options:

1. Click the **Default Storage** tab.
2. In the **Resource manager** field, select a default resource manager from the list.
3. In the **Collection** field, select a collection from the list. All objects identified by this item type are stored in the default collection.
4. In the **Prefetch collection** field, select a prefetch collection from the list for temporary storage. A prefetch collection is the z/OS term for a staging area.
5. Click **OK** to close the window.

Important: If you select the default resource manager from one source, such as the user from either the user or the item type, and you select the default collection from the other source, such as the item type from either the user or the item type, you must create a collection with the same name in all the possible default resource managers defined for each user and item type.

You can later change the information on this window by selecting a part on the Default Storage page and clicking **Edit**.

Related concepts

“Resource manager” on page 41

“Collection” on page 360

Logging item type events

Logging is important, for example, because it tracks records needed for audit and security reasons.

To log item type events:

1. Click the **Logging** tab.
2. Select one or more check boxes to specify whether the library server logs an event when an item is created, read, updated, or deleted.
3. Select **Content retrieval** to enable event logging upon retrieval of content from the resource manager. This check box is available for document or resource item types only. When a user attempts to retrieve a whole or partial object from the resource manager, the event is logged to the system event table. This includes requests to export the object to third-party servers and requests to retrieve stream metadata to play in VideoCharger.

Restriction: When the library server requests the object from the resource manager for text-indexing purposed, the records will not be logged into the system event table.

Content retrieval events are not logged when content is requested from resource managers on z/OS.

This feature uses event code 531 to log object retrievals from an enabled resource manager. You can view the event codes in the ICMSTITEMEVENTS table.

Related concepts

“Event logging” on page 414

Related reference

“ICM library server event table log” on page 418

Defining document management relations

You associate document parts with a document item type. You can associate any given document part item type with only one document item type. You associate document parts with a document in the Define Document Management Relations window, which you reach by clicking **Add** on the Document Management page of the New Item Type Definition window.

When you associate document parts with a document, you can select one of five predefined document part item types: ICMANNOTATION, ICMBASE, ICMBASETEXT, ICMNOTELOG, and ICMBASESTREAM.

When you define a document item type with parts, the access control list (ACL) that is specified in the Define Document Management Relations window is used to govern access to the parts. This ACL overrides the ACL that is specified for the part item type and is unique for each combination of document and part item type.

To associate document parts with a document:

1. Click the **Document Management** tab from the New Item Type Definition window.
2. Click **Add** to open the Define Document Management Relations window.
3. In the **Part type** field, select a part to associate with the document item type.
4. In the **Access control list** field, select an access control list to associate with the part type.
5. In the **Resource Manager** field, select the resource manager on which the part type is stored.
6. In the **Collection** field, select the collection on which the part is stored. There are two predefined collections that you can use, or you can create your own collections. For Windows and UNIX, the predefined collections are TABLE.CLLCT001 and CBR.CLLCT001. TABLE.CLLCT001 is a BLOB (binary large object) collection. CBR.CLLCT001 is a file system collection.

Tip: Use the BLOB collection for collections of small objects. If you have large objects, for example ones that are primarily larger than 20 KB each, the file system collection will provide faster performance.

7. In the **New version policy** field, specify a version policy for the part type. If you click **Prompt to create**, the Client for Windows will prompt a user to create another version of an item or update the current version of an item when making changes. You can prompt the user when an item's notelog has been updated or when an annotation has been added, deleted, or changed. Select ICMANNOTATION as the part type for annotations and ICMNOTELOG as the part type for notelogs.
8. In the **Maximum total versions** field, specify the number of versions for the parts. When you reach the maximum versions specified, Content Manager EE removes the oldest version and stores the latest version.
9. Click **OK** to save the information and close the window.

After you make an association, you can select a specific association on the Document Management page and click **Edit** to open the Define Document Management Relations window and make a change. For example, you can associate a different access control list with a part type or modify the version policy for a part type. You can select a specific association and click **Delete** to delete the association, for example, if you specified the wrong part type. You cannot delete an association after you have stored items or you will lose parts.

Specifying user exit routines

User exit routines are standard sets of code defined by a client application. You can specify user exit routines to determine the processing the client application performs. On the User Exits page, you can set up a particular item type for these user exit routines. To specify user exits:

1. Click the **User Exits** tab.
2. In the fields, type the functions and the name of the DLL that contains those functions, to determine the processing that the client application performs when users save, search, and sort items of this item type. You can also specify the processing that occurs when users store objects on the resource manager.

Viewing or modifying an item type

On an existing item type, the attribute's default value can be modified. Depending on the data type of the attribute, you might be able to modify the minimum or maximum values. However, if the item type is already in use, changing the minimum or maximum value is not recommended.

Restrictions: If you have already defined an item type, you cannot:

- Modify the item type name.
- Modify the item type classification.
- Modify the media object (XDO) class.
- Enable a document part item type for auto-linking.
- Change a component type attribute from required to non-required or vice-versa.
- Change a component type attribute from unique to non-unique or vice-versa.
- Change a component type delete rule.
- Disable text search if you already enabled it.
- Change the CCSID (supported code page) for text search.
- Change the language code for text search.

The system administration client returns an error if you attempt to modify properties that cannot be modified. If you are working with the APIs, review the log files (ICMSERVER.log and dklog.log). The error message ICM70001 is normally returned by the library server when an update is not permitted.

Before you modify an item type definition, determine the best time to modify it. If you modify it when users are active, then users could create or update items based on the old item type definitions in their cache. This situation can cause the create or update action to fail, or it can cause problems for users who try to access the item later. Modify an item type during off-peak hours to reduce synchronization errors between items and item type definitions.

To view or modify an item type:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Item Types** to display all of the item types in the right pane.
3. Right-click the item type that you want to view or modify and click **Properties**. The Properties window opens.
4. View or modify the information. See “Item type” on page 156 for specific information about all of the fields.
5. Click **OK** to save the item type.

Copying an item type

To copy an item type:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Item Types** to display all of the item types in the right pane.
3. Right-click the item type that you want to copy and click **Copy**. The Copy window opens.
4. Change the name of the item type and the names of any child components in the item type. Change other information for the item type. See “Item type” on page 156 for specific information about all of the fields.
5. Click **OK** to copy the item type.

Deleting an item type

You cannot delete an item type that contains data. Deleting an item type deletes all the views associated with it.

Recommendation: Keep a list of the item types that you use in document routing processes, particularly those item types that you use in decision points or collection points. The library server does not restrict you from deleting item types that are used in decision points or collection points.

Forming relationships between items

Restriction: Most of the function described in this section is not supported by the Client for Windows or the eClient. For a complete list of what is supported by the provided clients, see Table 31 on page 128.

This section describes the various ways that you can form relationships between items in IBM Content Manager. IBM Content Manager provides links and references, and the underlying relational database provides foreign keys. Table 43 summarizes the linking mechanisms.

Table 43. Advantages and restrictions of linking mechanisms

Linking mechanism	Used at component level	Linked elements can be deleted	Versioning
Link	Root to root	Yes	No
Reference	Root or child to root	Specify when you create the reference	Specify when you create the reference
Foreign key	Root to a different item type or external table	Specify when you create the foreign key	Specify when you create the foreign key

Table 43. Advantages and restrictions of linking mechanisms (continued)

Linking mechanism	Used at component level	Linked elements can be deleted	Versioning
Hierarchical link	Root to root	Yes, the linked hierarchical element can be removed if it is an item, document, or folder if the element does not contain any hierarchical descendants	No

Beginning with Version 8.4.3, you can also form relationships between items by using the hierarchical data model to create hierarchical folders and documents. The hierarchical data model is a data model that mimics the structure of a file system, with documents and other items contained in a rooted folder hierarchy.

Related tasks

Working with hierarchical item types

Defining a link type

Define a link type to provide a custom link relationship that you can use in your custom client applications.

IBM Content Manager provides two link types: folder contains (DKFolder) and containment relationship (Contains). You can use the folder contains link to mimic the connection of a physical folder and a contained document. You can specify your own link types to symbolically represent the various links that are required for your data model.

To define a link type:

1. Expand **Data Modeling** in the system administration tree.
2. Right-click **Link Types** and click **New** to open the New Link Type window.
3. In the **Name** field, type up to 32 characters as the name for the link type.
4. In the **Display name** field, type a name that displays to end users in client applications. Click the **Translate** button, to open the **Translate Display Name** window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
5. Click **OK** to save the information and close the window.

Link

Create links to associate a source item and a target item, with an optional description item.

A *link* is a directional relationship at the root component level between two items: the source item and the target item. You can use links to associate one or more items with each other at the root component level at run-time. For example, assume that you have a Customer item and an Underwriter item, and you want to associate the two. Instead of making Underwriter a child component of Customer, you can associate the two by using a link.

In the system, you define a link, and the APIs create an entry in the links table to link the two items, as shown in Figure 18.

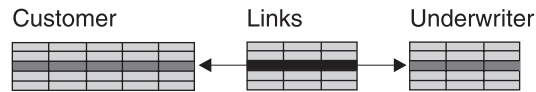


Figure 18. A link in action. Customer and Underwriter are root components of separate items; they are linked with a link that is specified in the links table.

As illustrated in the figure, the link is separate from the linked items. It is in a links table that contains information about which linked item is the source, which is the target, and the type of link. The link itself does not belong to either the source or the target.

IBM Content Manager provides two link types: folder contains and containment relationship. You can specify your own link types to represent the various links that are required for your data model. For the example shown in Figure 18, you might want to use a link that does not imply containment, so you might create your own simple connection link.

You can link only between root components of different items. As summarized in Table 43 on page 173, there are no restrictions on links, other than privileges; either the source or target can be deleted. The link is independent of versions.

Viewing a link type

Restriction: You can only modify the display name of a link type. To view a link type:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Link Types** to display the link types in the right pane.
3. Right-click a link type and click **Properties** to open the Properties window.
4. View the information.
5. In the **Display name** field, you can modify the name that displays to end users in client applications. Click the **Translate** button, to open the **Translate Display Name** window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
6. Click **OK** to save the information and close the window.

Copying a link type

To copy a link type:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Link Types** to display all of the link types in the right pane.
3. Right-click the link type that you want to copy and click **Copy** to open the Copy window.
4. In the **Name** field, type up to 32 characters as the name for the link type.
5. In the **Display name** field, type a name that displays to end users in client applications. Click the **Translate** button, to open the **Translate Display Name** window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
6. Click **OK** to save the information and close the window.

Deleting a link type

Restriction: You cannot delete a link type if it is being used.

To delete a link type:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Link Types** to display the link types in the right pane.
3. Right-click the link type you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

Creating a reference attribute

You can use a reference attribute to point to specific information contained in another item.

To create a reference attribute:

1. Expand **Data Modeling** in the system administration tree.
2. Right-click **Reference Attributes** and select **New** to open the New Reference Attribute window.
3. In the **Name** field, enter a descriptive name for the reference attribute.
4. In the **Display name** field, enter a name that displays to end users in client applications.
5. Click **Translate** to open the Translate Display Name window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information and return to the New Reference Attribute window.
6. Click **OK** to create the reference attribute.

Reference attribute

A *reference* is a single-direction, one-to-one association between a root or child component of an item and a root component of another item of the same or different item type. For example, assume that you have a personal auto policy root component with an Insured vehicles child component and an Operators child component. You also have an Underwriter root component that you want to associate with certain Claims that are under the Customer root component. In IBM Content Manager, you can associate the Claims child component with the Underwriter root component by using a reference, which is shown as the arrow in Figure 19.

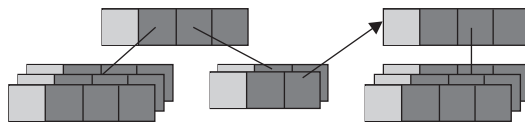


Figure 19. A reference in action

In the system, you define the reference as an attribute that is part of the source item.

You can use a reference attribute to point to specific information contained in another item.

IBM Content Manager reference attributes have the following rules:

- The target of the reference attribute must be the root component of an item.
- If there is more than one reference attribute in the same component type, they must have the same delete rule. You establish delete rules when you create the reference attribute.
- You can create a circular reference. For example, itemA references itemB, which references itemC, which references itemA.
- When updating a target item, and thus removing the oldest version of the target item, you might receive an error if the delete rule on the source attribute is set to restrict or no action.
- You can delete the target item of a reference attribute if all of the following conditions are met:
 - The item is not a target item for another reference attribute. However, you can delete it as long as the delete rule is not set to "restrict" or "no action" for all the references attributes that have the deleted item as a target.
 - The item is not checked out.
 - You have the correct privileges.
 - If the delete rule is set to cascade, the number of components remains above the minimum cardinality.

You can create a reference to associate a root or child component of one item to the root component of another item. Table 43 on page 173 shows that when you create the reference, you can determine whether the target can be deleted if there is any reference to it.

Related concepts

Links and references

Related tasks

“Creating a reference attribute” on page 176

“Viewing or modifying a reference attribute”

“Copying a reference attribute” on page 178

“Deleting a reference attribute” on page 178

Viewing or modifying a reference attribute

To view or modify a reference attribute:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Reference Attributes** to display all of the reference attributes in the right pane.
3. Right-click the reference attribute that you want to view or modify and click **Properties**. The Reference Attribute Properties window opens.
4. In the **Display name** field, enter a name that displays to end users in client applications.
5. Click **Translate** to open the Translate Display name window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information and return to the Reference Attribute Properties window.
6. Click **OK** to save the reference attribute.

Related concepts

“Reference attribute” on page 176

Related tasks

“Deleting a reference attribute”

“Viewing or modifying an attribute” on page 150

“Deleting an attribute” on page 150

Copying a reference attribute

To copy a reference attribute:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Reference Attributes** to display all of the reference attributes in the right pane.
3. Right-click the reference attribute that you want to copy and click **Copy**. The Copy Reference Attribute window opens.
4. In the **Name** field, enter a new descriptive name for the reference attribute.
5. In the **Display name** field, enter a name that displays to end users in client applications.
6. Click **Translate** to open the Translate Display name window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information and return to the Copy Reference Attribute window.
7. Click **OK** to save the reference attribute.

Deleting a reference attribute

Restriction: You cannot delete a reference attribute if it is currently used in an item type.

To delete a reference attribute:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Reference Attributes** to display all of the reference attributes in the right pane.
3. Right-click the reference attribute that you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

Related concepts

“Reference attribute” on page 176

Defining a foreign key

The foreign key constraint in databases can be used within IBM Content Manager to define a relationship between an IBM Content Manager item type attribute and another attribute either within or external to IBM Content Manager.

When you define a foreign key in a database, you establish a relationship from a key in one table to a unique or primary key in another table to enforce referential integrity among database tables. In IBM Content Manager, you can define a foreign key relationship between an IBM Content Manager item type attribute and an attribute in another item type. You can also define a foreign key relationship between an IBM Content Manager item type attribute and a separate database table and column external to IBM Content Manager, enforcing similar integrity

rules. For example, you can use foreign keys to limit the values that users can enter for an attribute by populating the client indexing interfaces with drop-down lists of values.

To define a foreign key:

1. Expand **Data Modeling** in the system administration tree.
2. Right-click **Item Types** and click **New** to open the New Item Type Definition window.
3. Click the **Foreign Keys** tab.
4. Click **Add** to open the Define Foreign Key window.
5. In the **Constraint name** field, type a name for the tie between the attributes. This name also becomes the constraint name in the database.
6. In the **Update rule** field, select **Restrict** so that the target cannot be updated. If you select **No action**, the target can be updated.
7. In the **Delete Rule** field, select one of the following options:
 - **Restrict** so that you cannot delete the target because it is referenced by the source
 - **No action** so that you cannot delete the target because it is referenced by the source

Attention: Beginning with Version 8.4.2, the **Cascade** and **Set null** delete rule options for a foreign key are deprecated and are no longer available for selection when you define a foreign key in a new item type definition. The **Cascade** delete rule option means that when the target is deleted, the source is deleted. The **Set null** delete rule option means that when the target is deleted, the source is set to null.

If you used one of these options in an item type definition that was created with an earlier version of the product, check your existing foreign key delete rules and edit them to use a nondeprecated option instead. The foreign key delete rules configure actions that are done by the database manager and that bypass the IBM Content Manager checks such as access control lists (ACLs). If you allow these deprecated options to remain in your older item type configurations, you might lose data or create orphaned objects in the resource manager.

If you currently have custom applications that are based on the application programming interfaces (APIs) and these deprecated options are used in the custom applications to define a foreign key delete rule, the library server returns an error message stating that the nondeprecated options must be used. The error message is logged in the library server log file, ICMSEVER.log by default.

8. Select the source item type or child component from the **Select source component** list.
9. In the **Select target Item Type or table** field, select whether to use another IBM Content Manager item type as the target, or use an external table. If you select an external table, type the schema and name of the target table.

Restriction:

- You cannot select a target item type (parent table) that is enabled for versioning because creating a foreign key requires a unique constraint, and unique constraints are not supported for item types that are enabled for versioning.

- The feature that supports the display of foreign key attributes as choices in eClient indexing interfaces such as drop-down fields does not support values from external tables. The eClient can read foreign key values from IBM Content Manager item types only. However, the referential integrity of the constraint is enforced for external tables, even if the value does not display in the interface.

10. Select the attributes that you want to pair.

For this type of target	Perform this action
IBM Content Manager item type target	Select attributes from the Source attributes and Target attributes lists and click Add to pair the source and target attributes.
An external table target	Select an attribute from the Source attributes list and type a column name in the Target column field. Click Add to pair the source attribute and target column.

Restriction: To create a foreign key definition, you must use required attributes in the target item types. You can define an attribute as required when you associate it with the item type on the **Attributes** page of the New Item Type Definition window.

11. Select the **Show target data as dropdown in client** check box to have the target information displayed in the eClient or other custom applications.

In the eClient, if a relationship exists between two attributes, then the initial presentation to the user is to select a value in the parent drop-down list and display the corresponding values in the dependent drop-down list. When another selection is made in the parent field, then the page submits a refresh action to the servlet and gets a new set of values for the dependent field. The attribute relationships can be multiple layers deep.

For example, State is dependent on the selection of the Country attribute. The initial page displays all of the values for the Country attribute and the State drop-down list is pre-filled with values based on the first Country value in the list. When a new selection is made in the Country drop-down list, the form is populated again with a new set of State values, after first removing the previous values.

The predefined value function is only supported in the root component attributes and not in child component attributes.

Foreign key restraint to external database tables is supported in the system administration client, but the external database values are not returned to the end user application.

12. Click **OK** to save the information and close the window.

Tip: After you define a foreign key, you can change its characteristics. On the **Foreign Keys** tab, select a foreign key entry and click **Edit** to open the Define Foreign Keys window. Then, for example, you can change the pairing between source and target attributes.

“Foreign key” on page 181

“Foreign key example: Linking between IBM Content Manager attributes” on page 181

“Foreign key example: Linking between IBM Content Manager and an external database table” on page 184

Foreign key

You use a foreign key to establish a relationship with a unique key or the primary key to enforce referential integrity among tables.

Foreign keys are constraints supplied by the underlying database management system. A *foreign key* is a column or a set of columns in a table that refer to a unique key or the primary key of the same or another table. A *unique key* is a column or a set of columns for which no values in a row are duplicated in any other row. You can define one unique key as the *primary key* for the table. Each table can have only one primary key.

In IBM Content Manager, you can define foreign keys to another item type or to a database table that is not part of the IBM Content Manager system. For example, you might have a database table that is not part of the IBM Content Manager system. This database table contains a list of account numbers. You also have an item type in the IBM Content Manager system for account-related documents. You can create a connection between the account-related item type and the account number table by using a foreign key. By doing so, you ensure that the account-related documents always contain valid account numbers.

Restriction: You cannot create foreign key with a target item type that is enabled for versioning because creating a foreign key requires a unique constraint on the target column, and unique constraints are not supported for item types that are enabled for versioning.

Foreign key example: Linking between IBM Content Manager attributes

The goal of this example is to create a foreign key between attributes of two IBM Content Manager item types and to demonstrate that the foreign key constraint is used as expected in the IBM Content Manager clients.

Important: This example provides steps that are essential to accomplish the goal of the example. However, this example does not provide the complete steps for all procedures. For example, steps to save the new attributes and item types are not explicitly documented because they are considered to be understood by knowledgeable IBM Content Manager users.

Creating attributes, item types, and a foreign key

A system administrator who is responsible for the data modeling for the business creates attributes, item types that use these attributes, and a foreign key that links between the attributes to provide referential integrity across items created with the item types. The process flow for these tasks includes the following steps:

Create the attributes: Create two attributes, a FormId attribute to hold the identifier (ID) for a type of form, and a FormName attribute to hold the text description of the form type.

1. From the IBM Content Manager system administration client navigation tree, expand **Data modeling**, right-click **Attributes**, and click **New**.
2. Create an attribute with a **Name** and **Display name** of FormId. Select **Character** as the Attribute type with **Alphanumeric** as the Character type. In the **Length** field, enter 8.
3. Create an attribute with a **Name** and **Display name** of FormName. Select **Variable Character** as the Attribute type with **Alphanumeric** as the Character type. In the **Length** field, enter 32.

Create the first item type: Create a FormType item type to contain the form types that will be added as items. Add the FormId attribute to the item type to store the IDs of form types. Add the FormName attribute to the item type to store the descriptions of form types. Prepare the FormId attribute to be used as part of the foreign key. Set the FormId to be a required attribute for the FormType item so that each form type has an ID. Set the FormId to be a unique attribute for the FormType so that each ID is unique.

1. From the system administration client, right-click **Item types** and click **New**.
2. On the Definition page, enter FormType for the **Name** and **Display name** fields. In the **Item type classification** field, select **Document**.
3. On the Attributes page, add the FormId attribute to the item type. Select **Required** and **Unique** so that a unique ID is required for each form type. Select **Represents item** so that the FormId attribute is displayed in the client to represent the FormType item.

Tip: An attribute must be set as required on the item type to be used as a foreign key.

4. Also on the Attributes page, add the FormName attribute to the item type. Select **Required** and **Unique** so that each form type requires a unique description.
5. On the Document Management page, add the ICMNOTELOG document part so that users can enter comments about the items in this item type. Because this item type is used as a folder to define types of forms and is not used to store documents, this part is the only part needed for the item type.

Create the second item type: Create a Forms item type to contain the individual forms that will be added as items. Add the FormId attribute to the item type so that it is common to both item types so that it can be used as the foreign key constraint between the FormType item type and the Forms item type.

Tip: It is not required to use the same attribute as the source and target attribute of the foreign key. The same attribute is used in this example for illustrative purposes.

1. From the system administration client, right-click **Item types** and click **New**.
2. On the Definition page, enter Forms for the **Name** and **Display name** fields. In the **Item type classification** field, select **Document**.
3. On the Attributes page, add the FormId attribute to the item type. Select **Required** to indicate that this is a required attribute for all Forms items.
4. Also on the Attributes page, add other attributes that are commonly needed for a document item type, for example, a timestamp or owner name.
5. On the Document Management page, add document parts that are commonly needed for a document item type, for example, ICMANNOTATION, ICMBASE, and ICMBASETEXT.

Create the foreign key on the second item type: As part of the creation of the Forms item type, create a foreign key constraint with the Forms item type as the source item type and the FormType item type as the target item type. Set the FormId attribute as the source attribute and target attribute. In the foreign key relationship, the source is constrained by the target. Therefore, the values available to the FormId attribute in the Forms item type are limited by the values available in the FormId attribute in the FormType item type.

1. On the Foreign Keys page of the Forms item type definition, click **Add**.

2. In the **Constraint name** field of the Define Foreign Key window, enter `FormIdConstraint`.
3. Select **Restrict** for the **Update rule** and select **Restrict** for the **Delete rule**.
4. Choose the source and target item types for the foreign key. For **Select source component**, select the **Forms** item type. For **Select target Item Type or table**, select **Use Content Manager Item Type** to use an IBM Content Manager item type as the constraint. For **Select target Item Type**, select the **FormType** item type.
5. Select the attributes on the source and target that reference each other. For **Source attributes**, select **FormId**. For **Target attributes**, select **FormId**. Select **Show target as dropdown in client** to enable the target attribute from the **FormType** item type to show as a drop-down field in the clients.

Creating items in the FormType item type

A business analyst who is responsible for creating the objects for the business creates the form types in the **FormType** item type. This action includes assigning IDs to the form types by using the **FormId** attribute. The business analyst creates two new form items with the **FormFolder** item type, a medical insurance application with the form ID 1A100001 and a medical claim form with the form ID 1A100002. The process flow for these tasks includes the following steps:

1. From the eClient, click **Create Folder**.
2. In the **Item Type** list, select **FormType**. In the **FormId** field, enter 1A100001 as the form ID. In the **FormName** field, enter Medical Insurance Application as the descriptive form name.
3. In the **Item Type** list, select **FormType**. In the **FormId** field, enter 1A100002 as the form ID. In the **FormName** field, enter Medical Claim Form as the descriptive form name.

Importing an item to IBM Content Manager

Users who are responsible for importing the forms into the content management system work with forms according to the normal business process, such as importing scanned documents. When a user imports a form, the user assigns an ID that defines the type of form that is imported. The client that is used to import the document limits the values for the ID by using the foreign key constraint. The client might limit the values directly in the interface by using the acceptable values in a drop-down menu, or the client might limit the values indirectly by verifying the supplied value on the library server.

For example, a user imports a form with the eClient. The eClient can display the IBM Content Manager foreign key item types and attributes in the interface. Therefore, the user can select **Forms** from the **Item type** field and select an ID from a **FormId** drop-down list. The **FormId** list contains only the IDs entered by the business analyst as the **FormId** values for the **FormType** item type.

Other client applications might not display the foreign key values for selection. For example, the Client for Windows does not display the values from foreign keys by default. In addition, a custom client application might not be designed to show these values. However, regardless of the client that is used, the foreign key referential integrity is enforced by the library server.

For example, a user imports a form with the Client for Windows, using the **Forms** item type. Because a **FormId** drop-down list does not display in the Client for

Windows, the user enters an ID value manually. The ID contains a typographical error, such as 1AA00001 when the valid IDs are 1A100001 and 1A100002. The resulting entry is not defined as a FormId in the FormType item type. When the user imports the form, the following error message is shown: The system could not create a document object. The error details contain IBM Content Manager and SQL error codes to help the user work with the system administrator. The error codes show that the value for the dependent table (the FormId attribute of the Forms item type) does not match any value of the parent key in the parent table (the FormId attribute of the FormType item type).

Result

In this example, attributes and item types were created in IBM Content Manager. A foreign key relationship was created between two item types. An attribute that was used in both item types was configured as a foreign key to constrain the values of the attribute from one item type to another. The values were displayed in the eClient interface to limit the values that users could select when creating items. In addition, other client applications that could not display the values still used the foreign key to enforce referential integrity between the two item types.

Foreign key example: Linking between IBM Content Manager and an external database table

The goal of this example is to create a foreign key between an item type attribute in an IBM Content Manager database table and data in an external database table in a different database and to demonstrate that the foreign key constraint is used as expected in the IBM Content Manager clients.

Important: This example provides steps that are essential to accomplish the goal of the example. However, this example does not provide the complete steps for all procedures. For example, steps to save the new attributes and item type are not explicitly documented in the example because they are considered to be understood by knowledgeable IBM Content Manager users.

Preparing the external database table to use the foreign key

The database administrator for the external database table and the IBM Content Manager library server database ensures that the data from the external database table is directly accessible by the library server. The external database table must meet these requirements:

- It must be in the same database as the library server.
- It must grant read privileges for any IBM Content Manager user. These users include icmadmin (the default library server administration user ID), icmconct (the default database connection user ID), and any other IBM Content Manager users who connect to the database.

In this example the external database table is in a different database, so the table does not meet the requirement that it must be in the same database as the library server. Therefore, the database administrator re-creates the external database table on the library server. To ensure that the data is synchronized, the database administrator creates a utility that copies data from the original external database table to the duplicate of the external database table on the library server.

Important: If you use this method to copy data to the library server database, do not modify any IBM Content Manager library server database tables, and ensure that the copied tables do not conflict with IBM Content Manager library server tables.

For example, the external database table that is not available to the library server holds data about customers, including each customer name and account number. On the library server DB2 database, the database administrator creates a duplicate DB2 table with the name ACCOUNTLIST to hold the list of customer accounts. The ACCOUNTLIST table has two columns. The ACCOUNTNUM column holds customer account numbers and the ACCOUNTNAME column holds the customer names. The ACCOUNTNUM column is defined as a primary key so that it can be used as part of a foreign key constraint. The database administrator enters the following SQL command in the library server database to do this task:

```
CREATE TABLE ACCOUNTLIST ( ACCOUNTNUM CHAR (8) NOT NULL PRIMARY KEY,
ACCOUNTNAME VARCHAR (32) NOT NULL )
```

Tip: This example **create table** command is compatible with both DB2 and Oracle database servers.

After the duplicate table is created, the custom utility created by the database administrator copies the data from the external database table to the duplicate database table on the library server. In this example, two customers are in the account list of the ACCOUNTLIST table, ExampleCo. Enterprises and ExampleCo. LLC. The populated table appears as follows:

ACCOUNTNUM	ACCOUNTNAME
123-4567	ExampleCo. Enterprises
222-3333	ExampleCo. LLC

Creating an attribute, an item type, and a foreign key in IBM Content Manager

The system administrator who is responsible for the data modeling for IBM Content Manager creates attributes, item types that use these attributes, and a foreign key that links between an IBM Content Manager attribute and a column in the duplicate of the external table to provide referential integrity between the item type and the duplicate of the external table. The process flow for these tasks includes the following steps:

Create the attribute: Create an attribute, AccountNum, to hold the account numbers for customers.

1. From the IBM Content Manager system administration client navigation tree, expand **Data modeling**, right-click **Attributes**, and click **New**.
2. Create an attribute with a **Name** and **Display name** of AccountNum. Select **Character** as the Attribute type with **Alphanumeric** as the Character type. In the **Length** field, enter 8.

Create the item type: Create an AccountDocument item type to contain documents about customer accounts. Add the AccountNum attribute to the item type to contain customer account numbers. Prepare the AccountNum attribute to be used as part of the foreign key. Set the attribute to be required so that the account number must be part of the customer document.

1. From the system administration client, right-click **Item types** and click **New**.
2. On the Definition page, enter AccountDocument for the **Name** and **Display name** fields. In the **Item type classification** field, select **Document**.
3. On the Attributes page, add the AccountNum attribute to the item type. Select **Required** so that an account number is required for each account document. Select **Represents item** so that the AccountNum attribute is displayed in the client to represent the AccountDocument item.

Tip: An attribute must be set as required on the item type to be used as a foreign key.

4. On the Document Management page, add document parts that are commonly needed for a document item type, for example, ICMANNOTATION, ICMBASE, and ICMBASETEXT.

Create the foreign key on the item type: As part of the creation of the AccountDocument item type, create a foreign key constraint with the AccountDocument item type as the source item type and the ACCOUNTLIST table as the target external table. Set the AccountNum attribute as the source attribute and set the ACCOUNTNUM column in the ACCOUNTLIST table as the target attribute. In the foreign key relationship, the source is constrained by the target. Therefore, the values available to the AccountNum attribute in the AccountDocument item type are limited by the values entered in the ACCOUNTNUM column of the ACCOUNTLIST table.

1. On the Foreign Keys page of the Forms item type definition, click **Add**.
2. In the **Constraint name** field of the Define Foreign Key window, enter AccountNumConstraint.
3. Select **Restrict** for the **Update rule** and select **Restrict** for the **Delete rule**.
4. Choose the source item type and target table for the foreign key. For **Select source component**, select the **AccountDocument** item type. For **Select target Item Type or table**, select **Use external table**. For **Schema**, enter ICMADMIN, the default name of the database on the library server, as the schema. For **Target table**, enter ACCOUNTLIST.
5. Select the attribute on the source and the table column on the target that reference each other. For **Source attributes**, select **AccountNum**. For **Target column**, enter ACCOUNTNUM.

Importing an item to IBM Content Manager

Users who are responsible for importing customer documents such as orders and invoices into the content management system work with forms according to the normal business processes, such as importing scanned documents. When a user imports a customer document, the user assigns the customer account number to that document. The client that is used to import the document limits the values for the account number by using the foreign key constraint. The client limits the values indirectly by verifying the supplied value with the values in the ACCOUNTNUM column in the ACCOUNTLIST table.

For example, a user imports an invoice for the ExampleCo. LLC customer in the Client for Windows. The IBM Content Manager clients cannot display foreign key values from external tables, so the user must enter the account number, 222-3333, manually. The account number contains a typographical error because the user enters 2223333 and forgets the dash (-). The resulting entry is not found in the ACCOUNTNUM column in the external ACCOUNTLIST table. When the user imports the document, the following error message is shown: The system could not create a document object. The error details contain IBM Content Manager and SQL error codes to help the user work with the system administrator. The error codes show that the value for the dependent table (the AccountNum attribute of the AccountDocument item type) does not match any value of the parent key in the parent table (the ACCOUNTNUM column in the external ACCOUNTLIST table).

Result

In this example, a duplicate of an external database table was created in the same database as the library server so that its columns could be used in a foreign key relationship. An attribute and item type was created in IBM Content Manager. A foreign key relationship was created between the IBM Content Manager item type and the duplicate of the external database table. An attribute from the item type and a column from the duplicate table were configured as a foreign key to constrain the values of the attribute by using the values from the duplicate table. Client applications that could not display the values still used the foreign key to enforce referential integrity between the item type and the duplicate table.

Enabling auto-linking

Auto-linking sets up attribute and attribute group associations across item types.

To enable auto-linking for new and existing item types:

1. Optional: On the Auto-linking page of the New Item Type Definition notebook, select the **Only show available matching attributes and groups** check box to ensure that only attributes and attribute groups at the same level are displayed.
2. Select an item type from the **Item type to be linked to** list. A list of attributes and attribute groups for that item type displays.

Restriction: Only certain item types can be used as the source item types in an auto-linking rule:

- If the target item type is a hierarchical item type, then the source item type cannot be a hierarchical item type.
 - A document part item type cannot be used as a source item type.
3. Select attributes or attribute groups from the **Current item type** list and **Item Type to be linked to** list.

Restriction: The following rules define how you can use attributes and attribute groups in these lists:

- You cannot link decimal, date, timestamp, or time attributes.
- You can link only required attributes. You specify if an attribute is required on the Attributes page of the New Item Type Definition notebook.
- If the target item type is a hierarchical item type, then the ICM\$NAME attribute displays in the **Current item type** list. However, you cannot link this attribute to any attribute in the **Item Type to be linked to**. This restriction exists because the ICM\$NAME attribute exists only in a hierarchical item type and a hierarchical item type cannot be used as the source item type in an auto-linking rule.

You can create links between root and child components of different item types. If you have a link from root to root and child to root, the minimum cardinality must be greater than 0.

4. From the **Link type** list, select a link type to associate the attributes or attribute groups. All links between the item types must be the same type.
5. Click **Add** to create a link set and add the attributes to the **Associated attributes and groups** list.
6. From the **Item type linked to** list under **Associated attributes for link**, select an item type. All attributes from this item type that are linked to the current item type display in the **Associated attributes and groups** list.

7. Optional: To delete a link or change the link type, select the linked attribute in the lower table and click **Remove**. You can then recreate the link, as needed.
8. Optional: If you have a long list of linked attributes, you can use the **Move up** and **Move down** buttons to order or group the links together while viewing.

After item types are linked based on your auto-link definitions, the link remains even if you change the definition. If you change the link type in the **Link type** list after clicking **Add**, it has no effect on the auto-link definition. You must select the link type before clicking the **Add** button.

To change a link type of an existing auto-link definition, first click the **Remove** button, and then re-add the auto-link definition with the correct link type selected.

Important: During Auto-linking, if the source object, such as a folder, contains a child component that has a minimum cardinality value that is greater than zero, the source object's attributes are not automatically populated. In the IBM Content Manager system, when a source item is populated by a target item, default rows with default values are not inserted into the child component of the source item according to the specified cardinality. As a consequence, if the attributes of the source child component are also the target of another source item, the source of this specified child component attribute are still populated according to the default value of the child component. In this scenario, the child component is missing and the system does not have the information to complete the auto-link chain.

Related tasks

Creating a hierarchical item type

Auto-linking

IBM Content Manager provides auto-linking. (Earlier IBM Content Manager versions included a more restricted implementation of auto-linking called auto-folding; the implementation was restricted to folder linking only.)

With *auto-linking*, you can set up attribute and attribute group associations across item types so that when data is entered in the attribute or attribute group of one item type, it is also entered into the matching attribute or attribute group of another item type. The data type of the attribute can be character, variable character, integer, and small integer.

As you create item types, you can establish auto-linking to automatically link related item types. Existing item types can also have auto-linking enabled.

There are restrictions on the item types that can be used as source item types when you set up auto-linking:

- A hierarchical item type can only be the target item type of an auto-linking rule. Therefore, if you use the system administration client to set up an auto-linking rule for with a hierarchical item type as the target, then the client does not display any hierarchical item types as potential source item types.
- A document part item type cannot be used as the source item type of an auto-linking rule. Therefore, when you create an auto-linking rule for a target item type, the system administration client does not display any document part item types as potential source item types.

After item types are linked based on your auto-link definitions, the link remains even if you change the definition. If you change the link type in the **Link type** list after clicking **Add**, it has no effect on the auto-link definition. You must select the link type before clicking the **Add** button. To change a link type of an existing

auto-link definition, first click the **Remove** button, and then re-add the auto-link definition with the correct link type selected.

You cannot establish auto-linking with an item type that does not exist.

Auto-linking can be at the root or child component level, or both. Any items that are created using the specified item types are automatically linked. If an item of one of the auto-linked types does not exist, it is automatically created, for example, if you create a form that must auto-link with a folder that does not yet exist, the folder item is automatically created.

A root to root link is not required when creating a child to root link. It is not necessary to select at least one attribute on the root component when defining the auto-linking between root and child components. You can have the link defined with all of the link attributes from the child only.

One or multiple attributes can be linked, and one item type can map to an arbitrary number of item types.

When using the "folder contains" link type for auto-linking, add the auto-link rule to the item type that is the "content" of the folder. Set the **Linked to** field to the item type of the intended folder.

For auto-linking, both the source and target attributes must be set as required in the item type definition. The source is the folder and the target is the document. The attribute must be the same attribute on both the target and the source.

Additionally, there are requirements for source attributes depending on whether they are actively involved in the auto-linking or are passively involved. The attribute that is part of the link is *active* in the auto-linking. Other attributes of the item type, which are not part of the link, are *passive*. If a passive attribute on the source is required, it must have a default value to prevent errors.

Table 44. Summary of attribute requirements for auto-linking

Role in auto-linking	Source (folder)	Target (document)
Active in auto-linking	All of the following conditions must be met: <ul style="list-style-type: none">• Attribute must be required.• Attribute must be the same as on target.	All of the following conditions must be met: <ul style="list-style-type: none">• Attribute must be required.• Attribute must be the same as on source.
Passive in auto-linking	Either of the following conditions must be met: <ul style="list-style-type: none">• Attribute is not required.• Attribute is required and has a default value.	There are no special requirements.

Important: Auto-linking is possible for document item types that are enabled for versioning. You can enable versioning in the **New version policy for attributes** field in the New Item Type Definition window. The folder item type to be linked to must not be enabled for versioning. The links for the document item type are maintained using the attributes of the current version of the item.

Restrictions:

When defining an auto-link rule that involves a child component attribute linked to a source root attribute, the minimum cardinality for the child component must be set to 1. The maximum cardinality can be set to 1 or greater; however, it is the responsibility of the application to maintain the uniqueness of the source item types' attribute, if that attribute is, in fact, unique.

There are some restrictions for linking attributes. The linking attributes type cannot be **TIMESTAMP**. When defining an auto-folder link between two item types, you can have a root to root and child to root link concurrently, but the linking attribute cannot be the same for both root and child.

Related concepts

"Version policy" on page 157

Related tasks

Creating a hierarchical item type

Defining data model options

You have several optional tasks you can perform to improve the display, performance, and use of the data model.

Defining a semantic type

Define a semantic type to describe and distinguish the use and purpose of an item.

Use a semantic type to help client applications identify the behavior for that item.

To define a semantic type:

1. Expand **Data Modeling** in the system administration tree.
2. Right-click **Semantic Types** and click **New** to open the New Semantic Type window.
3. In the **Name** field, type up to 32 characters as a descriptive name for the semantic type.
4. In the **Display name** field, type a name that displays to end users in client applications. Click the **Translate** button to open the **Translate Display Name** window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
5. Click **OK** to save the information and close the window.

Semantic type

The *semantic type* is a descriptive attribute for an item that helps applications to identify the behavior (semantics) for that item. Client applications use the semantic type to distinguish the use and purpose of different items. For example, you might use a document item type to store a document and another document item type to store a folder. The semantic type distinguishes the document from the folder.

You specify the semantic type when you create an item, and the semantic type is stored as an attribute value. You can select one of the following seven predefined semantic types:

Annotation

Additions to, or commentary about, the main data; following the document metaphor, annotations include sticky notes, color highlights, stamps, and other graphical annotations on a document.

Base The fundamental content of an item that stores any type of content, including image, text, and audio.

Container

A generic container for other items.

Document

A document, usually containing one or more base (ICMBASE) parts and possibly an annotation (ICMANNOTATION) and a notelog (ICMNOTELOG) part.

Folder A folder for containing items or other folders.

History

A log of activities for the associated item, entered as text by the application. This semantic type is available only for migration from earlier IBM Content Manager versions.

Note A log of information entered by users. For example, indicating the reason that the insurance application was denied or instructions to the next reviewer of the document.

In addition to the seven predefined semantic types, you can create your own semantic types in your application.

Viewing a semantic type

Restriction: You can only modify the display name of the semantic type.

To view a semantic type:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Semantic Types** to display the semantic types in the right pane.
3. Right-click a semantic type and click **Properties** to open the Properties window.
4. View the information.
5. In the **Display name** field, you can modify the name that displays to end users in client applications. Click the **Translate** button to open the **Translate Display Name** window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
6. Click **OK** to save the information and close the window.

Copying a semantic type

To copy a semantic type:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Semantic Types** to display all of the semantic types in the right pane.
3. Right-click the semantic type that you want to copy and click **Copy** to open the Copy window.
4. In the **Name** field, type up to 32 characters as the name for the semantic type.
5. In the **Display name** field, type a name that displays to end users in client applications. Click the **Translate** button to open the **Translate Display Name** window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
6. Click **OK** to save the information and close the window.

Deleting a semantic type

To delete a semantic type:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Semantic Types** to display the semantic types in the right pane.
3. Right-click the semantic type that you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

Defining a MIME type

Define the MIME type to tell your application how to handle an object retrieved from the resource manager.

Restriction: Once created, a MIME type cannot be deleted.

To define a MIME type:

1. Expand **Data Modeling** in the system administration tree.
2. Right-click **MIME Types** and click **New** to open the New MIME Type window.
3. In the **Name** field, type the name of the MIME type.
4. In the **Display name** field, type the name that displays in client applications to end users.
5. Click **Translate** to open the Translate Display Name window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
6. In the **MIME type** field, type up to 512 characters to describe the MIME type, for example, image/jpeg.
7. In the **Suffixes** field, type up to 512 characters as the suffix for the MIME type, for example, jpeg. A suffix is common known as a file extension and is used in the client applications when downloading or exporting the files from IBM Content Manager.
8. In the **Valid functions** field, specify the function that might be performed on the MIME type. For example, you might enable a .doc MIME Type to be text searchable.
9. In the **Application name** field, enter an alternate application and path or relative path that a client might use to view a particular MIME type. Click **Browse** to select an application name from the file system.
10. In the **Application flag** field, you can define options for running the application.
11. Click **OK** to save the MIME type definition.

Related tasks

“Defining a display name” on page 149

Object

In IBM Content Manager, an *object* is any data entity that is stored on a resource manager in digital form. Objects can include JPEG images, MP3 audio, AVI video, and plain text files. For example, a few of the formats that are supported natively by IBM Content Manager are: Microsoft Word, Lotus WordPro, TIFF, and JPEG.

Objects are managed by items on the library server. The items contain the necessary information for describing and locating the objects. Using the items, users can create, retrieve, update, or delete objects.

MIME type

In IBM Content Manager, when you create an object, you specify its MIME type. When an object of that type is retrieved from the resource manager, your application reads the MIME type and determines how to handle the object. For example, if the MIME type for an object is GIF, your application might launch a Web browser to view the object.

A *MIME* (Multipurpose Internet Mail Extension) *type* is an Internet standard for identifying the type of object that is being transferred across the Internet. MIME types include many variants of text, audio, image, and video data.

The MIME type replaces the content class from earlier IBM Content Manager versions.

To properly handle the various types of data in IBM Content Manager, each object needs to be associated with a MIME type. Viewers need to know the MIME types for viewing certain documents. You must decide which data types IBM Content Manager can use by identifying them to the system.

Tip: The IBM Content Manager library server, resource manager, and Java and C++ APIs do not use the MIME type setting internally for any type of processing and do not set MIME types on objects. The association between an object and a MIME type is set by the user and can be used by an application such as the Client for Windows, the eClient, or a custom application. IBM Content Manager saves system-defined and user-defined MIME types in the library server database. IBM Content Manager also saves the association between each object and user-specified MIME type in the library server resource part tables, such as the ICMUT00300001 table, and in the resource manager RMOBJECTS table.

IBM Content Manager ships with some predefined MIME types, which you can view in the system administration client, that a client application can use. If you need to store data types not identified by the predefined MIME types, you have to add new ones. When you define a new MIME type, then you need to use the following naming convention: content type/subtype.

A content type describes the contents of a document and allows the application to identify which view to use to present the document. A subtype specifies a specific format for the document. For example, the MIME type `image/jpeg` describes a file as being an image file while the subtype identifies that file as being of JPEG format. Available content types include, but are not limited to, the following types:

audio Audio files like music or voice recordings. Examples include: `audio/basic` and `audio/mpeg`.

application

Binary files and specific applications like Lotus Word Pro (`application/vnd.lotus-wordpro`) or Lotus Freelance (`application/vnd.lotus-freelance`).

image Image files like photos and drawings. Examples include: `image/tiff` and `image/g3fax`.

text Text files that can handle several character sets in several languages like HTML and XML files. Examples include: `text/plain` and `text/html`.

video Video or animated files like MPEGs. Examples include: video/mpeg and video/quicktime.

If you need to construct a MIME type that is not a standard MIME type, then you can define it using the naming convention: content type/x-subtype, where subtype is the user-specific subtype. For example, WAV files are not considered a standard MIME type, so, the MIME type name looks like the following example: audio/x-wav.

Important: If you define a MIME type that is considered a standard MIME type, and you use x-, the application you use might not recognize the document. For example, if you have an image that is a GIF, your browser can display it if you use the MIME type image/gif. However, if you define the MIME type as being image/x-gif, the browser does not recognize the subtype x-gif, and therefore, cannot display the image.

When you define a MIME type, you can also provide the usable suffixes for it. Suffixes are also referred to as file extensions. Some applications use the suffix to identify the MIME type. Common suffixes are .pdf for Adobe Acrobat files and .htm for hypertext documents common on the Internet. Suffixes assist MIME types to identify what type of data can be viewed on which viewer. However, most applications recognize file formats and identify the appropriate viewer to view the MIME type, whether you specify a suffix or not.

To view the MIME types that come with IBM Content Manager, expand Data Modeling in the system administration client and click **MIME Types**. The right pane displays the predefined MIME types.

Viewing or modifying a MIME type

To view or modify a MIME type:

1. Expand **Data Modeling** in the system administration tree.
2. Click **MIME Types** to display all MIME types in the right pane.
3. Right-click a MIME type and click **Properties** to open the Properties window.
4. In the **Display name** field, type the name to display in client applications to end users.
5. Click **Translate** to open the Translate Display Name window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
6. In the **MIME type** field, type up to 512 characters to describe the MIME type, for example, image/jpeg.
7. In the **Suffixes** field, type up to 512 characters as the suffix for the MIME type, for example, jpeg.
8. In the **Valid functions** field, specify the function that might be performed on the MIME type. For example, you might enable a .doc MIME type to be text searchable.
9. In the **Application name** field, enter an alternate application and path or relative path that a client might use to view a particular MIME type. Click **Browse** to select an application name from the file system.
10. In the **Application flag** field, you can define options for running the application.
11. Click **OK** to save the information.

Creating a media object (XDO) class

Create an extended data objects, also known as media XDOs, to define and describe an object.

IBM Content Manager provides predefined media object classes: DKLobICM, DKStreamICM, DKTextICM, and DKVideoStreamICM. **Requirement:** If you create your own XDO class, it must be derived from DKLobICM or one of its descendants.

To create a media object class:

1. Expand **Data Modeling** in the system administration tree.
2. Right-click **Media Object Classes** and click **New** to open the Media Object (XDO) Class Properties window.
3. In the **Name** field, type your preferred name for the media object class.
 - Use DKLobICM to add, retrieve, update, and delete generic resource manager objects. This type represents the most generic form of the resource item type classifications and can contain any kind of data. You can use this type when the origin or type of the item is unknown or undesignated.
 - Use DKStreamICM to add, store, or update large streamable objects.
 - DKTextICM represents text data that is stored on an IBM Content Manager Version 8 resource manager and pointed to by an item on the library server. You can index this media type and search for it using IBM DB2 Version 7 Text Information Extender or IBM DB2 Version 8 Net Search Extender. **For Linux**, use Net Search Extender.
 - Use DKImageICM for images stored in any format.
 - DKVideoStreamICM represents streamable video data that is stored on a streaming server resource manager and pointed to by an item on the library server.
4. In the **Description** field, type a description. For example, type ICMVideoStreamObject.
5. From the **Attribute group** list, select an attribute group to assign to the media object class.
6. In the **Java class name** field, type the Java class that handles the media object class.
7. If a C++ class handles the media object class, in the **DLL or shared object** field, type the name of the DLL that manages the media object class.
8. In the **Operating system** field, select an operating system associated with the media object class from the list.
9. If a C++ class handles the media object class, in the **Compilation type** field, select **Debug** or **Non-debug**. If you select **Debug**, debugging information is provided at run time.
10. Click **Add**.
11. Click **OK** to create the media object class and close the window.

Media object class

The *media object class* describes the data that is contained in an object and how to act on it. When you create an object type, you specify its media object class. When an object of that type is retrieved from the resource manager, your application uses the specified media object class to appropriately handle the object.

IBM Content Manager provides the following four predefined media object classes:

DKImageICM

Represents image resource objects in the resource manager configured for IBM Content Manager. A resource object consists of content stored in a resource manager and the metadata describing the content stored in the IBM Content Manager library server. Use DKImageICM for images stored in any format.

DKLobICM

Represents an abstraction for a generic large object (LOB) that is stored on a resource manager and pointed to by an item on the library server. Use DKLobICM to add, retrieve, update, and delete generic resource manager objects. To work with more specific types of data, you can use one of the more specific subclasses of DKLobICM: DKStreamICM, DKTextICM, and DKVideoStreamICM.

Some MIME types are inherently streamable, and so are appropriate for use with the DKStreamICM and DKVideoStreamICM media object classes. Other MIME types are text-searchable and are appropriate for use with DKTextICM. All MIME types can be stored as DKLobICM.

DKStreamICM

Represents generic streamable data that is stored on a resource manager and pointed to by an item on the library server. Use this class to:

- Add, store, or update large streamable objects from external sources using protocols such as FTP. The adding or storing of objects can be synchronous or asynchronous.
- Retrieve (synchronously or asynchronously) large streamable objects to external destinations.
- Specify where to begin and end streaming.
- Retrieve information about stream duration, rate, format, and group.

This class is a subclass of DKLobICM.

DKTextICM

Represents text data that is stored on an IBM Content Manager Version 8 resource manager and pointed to by an item on the library server. You can make a DKTextICM object text searchable by indexing the content of the object.

This class is a subclass of DKLobICM.

DKVideoStreamICM

Represents streamable video data that is stored on a streaming server (in this case, IBM DB2 Content Manager VideoCharger) resource manager and pointed to by an item on the library server.

Because the content of DKVideoStreamICM objects is often large, you should complete add, update, and retrieve operations through third-party servers using a standard protocol such as FTP. After you retrieve the item from the library server, you can use this media object class to initiate a session to stream the content between the video server and player.

This class is a subclass of DKLobICM and inherits its methods from the DKStreamICM class.

For more information about these media object classes and how to use them in your application, see the *Application Programming Reference*.

In addition to the predefined media object classes, you can define your own media object classes in the Media Object (XDO) Class Properties window.

Viewing or modifying a media object (XDO) class

To view or modify media object classes:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Media Object Classes** to display a list of media object classes in the right pane.
3. Right-click a media object class and click **Properties** to open the Properties window.
4. In the **Description** field, type a description.
5. In the **Attribute group** field, assign an attribute group to the media object class.
6. In the **Java class name** field, type the Java class that handles the media object class.
7. In the **DLL or shared object** field, type the name of the DLL that manages the media object class.
8. In the **Operating system** field, select an operating system associated with the media object class from the list.
9. If a C++ class handles the media object class, in the **Compilation type** field, select **Debug** or **Non-debug**. If you select **Debug**, more debugging information is provided at run time.
10. Click **Add**.
11. Click **OK** to save the media object class and close the window.

Copying a media object (XDO) class

To copy a media object class:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Media Object Classes** to display a list of media object classes in the right pane.
3. Right-click the media object class that you want to copy and click **Copy** to open the Copy window.
4. In the **Name** field, type the new name of the media object class.
5. In the **Description** field, type a description.
6. In the **Attribute group** field, assign an attribute group to the media object class.
7. In the **Java class name** field, type the Java class that handles the media object class.
8. In the **DLL or shared object** field, type the name of the DLL that manages the media object class.
9. In the **Operating system** field, select an operating system associated with the media object class from the list.
10. If a C++ class handles the media object class, in the **Compilation type** field, select **Debug** or **Non-debug**. If you select **Debug**, more debugging information is provided at run time.
11. Click **Add**.
12. Click **OK** to save the media object class and close the window.

Deleting a media object (XDO) class

Restriction: You cannot delete a media object class if it is currently used in an item type.

To delete a media object class:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Media Object (XDO) Classes** to display the media object classes in the right pane.
3. Right-click the media object class that you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

Creating a database index

Database indexing is an optional performance enhancing feature so that searches can be performed faster. You can create a database index for particular attributes.

When a user creates an item type, IBM Content Manager creates one table for each component of that item type and automatically creates indexes. See “Automatically created database indexes” on page 199 for more information.

IBM Content Manager creates a database index in the index table space default that you specify during item type creation. If you do not specify a default table space, IBM Content Manager does not designate a table space for the index. The index is then created in a table space according to the default behavior of the underlying database management system. For Oracle, the index table space that you specify during an IBM Content Manager installation or update process is used for IBM Content Manager system indexes only. That table space is not used for user-defined indexes unless you specify it as the default when you create the item type.

Recommendation: Use a separate table space for user-defined indexes to avoid contention with IBM Content Manager system indexes. Also, be aware that Oracle might create internal indexes that might not be located in the table spaces that you define in IBM Content Manager. The names of these internal indexes begin with the "SYS_" prefix.

Tip: If you are creating a new index, the table space information that is displayed for the index is always correct. If you are viewing the properties of an existing index and the option to disable dynamic table space information is selected in the library server configuration, then the table space information that is displayed for the index might not be correct because it is not retrieved dynamically from the library server.

To create a database index:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Item Types**.
3. Expand an item type in the tree or right-click an item type and click **Database Indexes**. The root and child components of the item type are displayed.
4. Right-click the component that you want to create an index for and click **New** to open the New Database Index window.
5. In the **Name** field, enter a descriptive name for the database index. Refer to the following guidelines when entering the name:
 - Use a maximum of 15 characters.

- Start the name with a letter.
 - You can include uppercase letters, numbers, and underscores.
 - You cannot use a reserved word.
6. Select the **Index keys are unique** check box to specify that the attributes are unique. For example, you can make an index containing Product IDs and mark it unique so that none of the Product ID values are duplicated.

Important: If the index contains more than one attribute, then it is the combination of all attributes that is enforced as unique. The uniqueness for each attribute in an index that contains multiple attributes is not enforced by using this option. For example, if you select this check box for an index that contains the Product IDs attribute and the Suppliers attribute, then the index could contain duplicate instances for a product in Product IDs and for a supplier in Suppliers. However, the index would contain only one instance for the combination of a particular product in Product IDs and a particular supplier in Suppliers.

7. In the **Available attributes** list, the attributes for the item type are displayed. Click **Add** to move them into the **Assigned attributes** list.
8. In the **DB2 storage/retrieval** field, specify the order for the attributes.
9. Click **OK** to create the database index.

Restriction: You cannot modify a database index.

For more information, see Index performance tips in the DB2 Information Center.

Related tasks

“Setting default table spaces for item type components, indexes, and LOB attributes” on page 166

“Setting default table spaces for item type components for Content Manager for z/OS” on page 167

Automatically created database indexes

When a user creates an item type, IBM Content Manager creates one table for each component of that item type and automatically creates indexes to enhance performance so that searches can be performed faster.

When the item type contains unique attributes, IBM Content Manager uses these indexes as part of the process to enforce uniqueness and also to ensure that the value of the attribute is unique among component IDs.

As a result of these automatically created indexes, any later attempts to create another component index on the same unique attribute fails with an error indicating that an index with the same definitions has already been created.

You can use the system administration client to list the indexes that are created for the item type.

Before IBM Content Manager Version 8.4 Fix Pack 1, IBM Content Manager created a unique constraint on the unique attribute. This unique constraint causes failure when the version policy for the item type is converted from Never create to either Always create or Prompt to create, eventually causing failure when creating or updating new versions.

With IBM Content Manager Version 8.4 Fix Pack 1 and later, this unique constraint is not created for new item types, and is deleted when the item type version policy is converted from Never create to either Always create or Prompt to create.

Related concepts

"Version policy" on page 157

Viewing a database index

Tip: When you view information about a database index, the name of the database index might contain the "NU" suffix on the end of the database index name. This suffix identifies a non-unique database index. Unique database indexes do not contain a suffix on the index name.

Restriction: You cannot modify a database index.

To view a database index:

1. Expand **Data Modeling** in the system administration tree.
2. Click **Item Types**.
3. Expand an item type in the tree.
4. Click **Database Indexes**. The root and child components of the item type are displayed.
5. Right-click a component and click **Properties** to open the Properties window.
6. Click **OK** to close the window.

Creating an item type subset

You can restrict which attributes users can view by creating item type subsets.

To create an item type subset:

1. Expand **Data Modeling** in the system administration tree.
2. Expand an item type in the tree.
3. Right-click **Item Type Subsets** and click **New** to open the New Item Type Subset window.
4. In the **Name** field, enter a descriptive name for the item type subset.
5. In the **Display name** field, enter a name that displays to end users in client applications.
6. Click **Translate** to open the Translate Display Name window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
7. Select an access control list for the item type subset.
8. **Optional:** To create a new access control list, click **Create Access Control List** to open the Create ACL window. After creating the new ACL, you return to this window to complete creating subsets.
9. Select the available attributes that you want users to view and click **Add**.
10. Use the **Attribute filter for view** fields so that users can only see attributes with certain values.
11. Specify user exit routines to determine the processing the client application performs. See Specifying User Exits for more information.
12. Click **OK** to create the item type subset.

Related tasks

“Creating access control lists” on page 471

Item type subset

You can use an item type subset to show only a specified set of data to end users.

An *item type subset* is a view of an item type that shows a specified set of data (a subset) that is included in items of that item type. For example, you might create an item type to use for employee data. You might want certain employees to be able to view different portions of that data. For example, all employees might be able to access an employee's location and phone number, but only the employee's manager can access the employee's salary history. The regular employees and the managers are using different item type subsets to view the information that they have access to and that is of interest to them.

In the Client for Windows, as in earlier versions, the item type subset is called the item type view or view. Client for Windows users can see the views that they have access to on the Views page of the Preferences notebook.

In the underlying database, the item type subset is a view of database table columns. In Content Manager EE Version 8, you can provide an attribute value to filter the rows. With item type subsets, you can filter both the attributes and the rows of items that are available in an item type.

Important: There can be only one filter per component type and the filter condition can only be set to equality. If a component is filtered at one level, levels below that level are filtered as well, but not levels above it. There is a performance impact for using row-based filters, especially when performing complex queries that access several component types that have row filters.

Restriction: When defining an item type subset for an item type, you cannot ignore a component level. For example, if you have a root component, child component, and grandchild component, in order for your item type subset to include information from the root and grandchild, it must also include at least one attribute from the child component.

Viewing or modifying an item type subset

To view or modify an item type subset:

1. Expand **Data Modeling** in the system administration tree.
2. Expand an item type in the tree.
3. Click **Item Type Subsets** to display the item type subsets in the right pane.
4. Right-click an item type subset and click **Properties** to open the properties window.
5. In the **Display name** field, enter a name to display to end users in client applications.
6. Click **Translate** to open the Translate Display Name window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
7. Select an access control list for the item type subset.
8. Select the available attributes that you want users to view and click **Add**.
9. Use the **Attribute filter for view** fields so that users can only see attributes with certain values.

10. On the User exits page, type the functions and the name of the DLL that contains those functions to determine the processing that the client application performs when users search and sort.
11. Click **OK** to save the item type subset.

Copying an item type subset

To copy an item type subset:

1. Expand **Data Modeling** in the system administration tree.
2. Expand an item type in the tree.
3. Click **Item Type Subsets** to display the item type subsets in the right pane.
4. Right-click an item type subset and click **Copy** to open the Copy window.
5. In the **Name** field, enter a new descriptive name for the item type subset.
6. In the **Display name** field, enter a name that displays to end users in client applications.
7. Click **Translate** to open the Translate Display Name window. All of the available languages defined in the system are listed. In the **Translated Name** column, type the translated display name for the other languages. Click **OK** to save the information.
8. Select an access control list for the item type subset.
9. Select the available attributes that you want users to view and click **Add**.
10. Use the **Attribute filter for view** fields so that users can only see attributes with certain values.
11. On the User exits page, type the functions and the name of the DLL that contains those functions to determine the processing that the client application performs when users search and sort.
12. Click **OK** to copy the item type subset.

Defining text search options

You have several options to select when creating a text search.

“Defining text search options for DB2 for Linux, UNIX, and Windows”

“Defining text search options for DB2 for z/OS” on page 209

“Defining text search options for Oracle” on page 215

Defining text search options for DB2 for Linux, UNIX, and Windows

You can make attributes, resource items, and documents text-searchable from the system administration client.

Tip: In versions earlier than Version 8.4.3, you might have configured the ICMCCSID environment variable before indexing documents in the following languages:

- Arabic
- Chinese (Simplified or Traditional)
- Japanese
- Russian
- Thai
- Turkish

Beginning with Version 8.4.3, the ICMCCSID environment variable is deprecated. However, you should allow the environment variable to remain at the value that is currently set.

The text search update index operation for a document might end abnormally or take too long. This causes subsequent new documents not to be indexed. To prevent this problem, you can set a timeout value for stopping a text indexing task and enabling the system to continue text indexing the next document.

To define text search options:

1. Click the **Options** button on the New Item Type Definition page or Attributes Page to open the Text Search Options window.
2. If you want to use default values for all of the text search options, select **DEFAULT SYSTEM** in the **Copy settings from** field and click **Load**. Alternatively, select another entry from the list and click **Load** to copy that entry's values in the Text Search Options window.
3. Select the format to be indexed in the **Format** field. The DB2 Text Information Extender or Net Search Extender requires the format or type of text documents (such as HTML, XML, or ASCII) that you intend to search. This information is needed when indexing documents.
4. In the **CCSID** field, specify the supported code page (CCSID) that is used to create the text index. Documents can be indexed if they are in one of the supported code pages. For a list of code pages, see the IBM DB2 Universal Database: *Text Information Extender Administration and User's Guide* (SH12-6732), the IBM DB2 Universal Database: *Net Search Extender Administration and User's Guide* (SH12-6740) or the DB2 Universal Database Information Center.

Restriction: This option is available only for BLOB attribute text indexes and is not available for other content text indexes or attribute text indexes.

5. In the **Language code** field, specify the language code that is used to create the text index.
6. In the **Index update settings** fields, specify parameters to control the frequency at which the index is updated. Specifically, you can specify the number of changes to the index before the next update, the amount of time that passes before the update. The index is updated when both the specified number of changes has been made and the specified time has elapsed.

Recommendation: Leave the **Commit count** field blank. Setting it to a non-zero value might lead to performance degradation. Before you commit a change to the database, the database records a log file of changes that can be undone. When you commit the update, this log file is erased, making your updates to the database permanent. It is currently recommend that you do not set a commit count to commit updates to the database. See the DB2 Text Information Extender documentation for further information about this situation.

7. In the **Storage Options** fields, specify the directory on the library server where the index files are stored and the directory on the library server where temporary files are stored for indexing.
8. In the **User defined function name** field, select the name of a user-defined function for retrieving objects from the resource manager. If the content is in plain text format, select ICMfetchContent. If the content is rich content, such as Microsoft Word documents or Acrobat PDF documents, select ICMfetchFilter. Do not use ICMfetchFilter with objects that are plain text.

When defining text-searchable user attributes, do not specify user-defined functions for Character, Variable character and CLOB attributes. The user-defined function ICMfilter should be used for BLOB attributes that contain non-text content such as Microsoft Word or Acrobat PDF documents.

Important: If you receive a DGL5200A error with a return code of 107 during the creation of a text searchable item type, that error indicates that you might have used a character that was not an ASCII character or that was not in the single-byte character set in the directory names for the **Storage Options** fields. Use only ASCII characters and single-byte character set characters in these directory names.

9. In the **User defined function schema field**, enter the name of the database schema in which the user-defined function is defined. If you use one of the standard user-defined functions (ICMfetchContent or ICMfetchFilter), you do not need to specify a user defined function schema.
10. In the **Model definition** fields, specify parameters for a model that might describe what sections of the text are to be indexed. The model consists of the name, a model file and the CCSID of the contents of the file. The model type is defined by the **Format** selection at the top of the Options window.
DB2 Text Information Extender allows you to index and search text fields in a structured document. The document model defines which fields in the document are indexed and available for searching.
11. Click **OK** to save the information.

Tip: If you receive a DGL5203A error indicating that the password is invalid when updating text indexes, you can set the correct DB2 Text Information Extender or DB2 Net Search Extender user ID and password on the Features page of the Library Server Configuration window.

Related reference

"Language codes" on page 13

"Specifying code pages for phrased text search of Thai language content" on page 613



Outside in Technology: Supported File Formats

Related information



Supported territory codes and code pages

Updating and reorganizing the index:

When an item type is made text searchable, the content for the document or resource items must be fetched from the resource manager for text indexing. The content is fetched when the text index is updated. You can update the text index manually or configure the text index to update automatically.

The IBM DB2 Universal Database: *Text Information Extender Administration and User's Guide* (SH12-6732) or the IBM DB2 Universal Database: *Net Search Extender Administration and User's Guide* (SH12-6740) provides more detailed information about how to update and reorganize the index.

IBM Content Manager includes a sample program that can update and reorganize the index for you. There are Java and C++ versions of the program with file extensions .java and .cpp. The name of the program is **STextIndexUpdateICM**. You can manually update and reorganize the index with the following procedure.

Although you can use the **Index update settings** fields to control the frequency that the text index is updated, there are times when items are in a queue waiting to be updated. You can use the following command to immediately update the index:

```
Db2text UPDATE INDEX myindex
FOR TEXT CONNECT TO icmnlbdb USER icmadmin
USING password
```

where:

- *myindex* is the name of the index. If you are unsure of the index name, you can find out by entering the following query at a DB2 command prompt:

```
select indexname from db2ext.textcolumns
```
- *icmnlbdb* is the name of the default database. You must substitute the database name if you renamed it.
- *icmadmin* and *password* are the user ID and password for the IBM Content Manager administrator.

This command is useful when you have added several items to the system administration database and want to search them immediately.

If a text column is often updated, subsequent updates to the index can become inefficient. You can reorganize the index to improve performance. You can do this by entering the following command:

```
db2text update index myindex for text reorganize connect to icmnlbdb user
icmadmin using password
```

where:

- *myindex* is the name of the index. If you are unsure of the index name, you can find out by entering the following query at a DB2 command prompt:

```
select indexname from db2ext.textcolumns
```
- *icmnlbdb* is the name of the default database. You will need to substitute the database name if you renamed it.
- *icmadmin* and *password* are the user ID and password for the IBM Content Manager administrator.

In the **Features** page of the **Library Server Configuration** window, you can set a timeout value. The timeout value can stop a text indexing task that might be taking too long or that has ended abnormally. Setting this timeout option allows the system to continue text indexing the next document.

Correcting text indexing failures:

When an item type is made text searchable, the content for the document or resource items must be fetched from the resource manager for text indexing. The content is fetched when the text index is updated. When the text index is updated, failures can occur when the system fetches the contents from the resource manager. If a failure occurs on one item, the item is not indexed, but text indexing continues.

Finding problems by using the UDFTRACEFILENAME trace file

Beginning with IBM Content Manager Version 8.4.2, the ICMSTSYSCONTROL system control table contains library server system configuration parameters for a trace file name and a trace level for the update text index function for the text search of objects on the DB2 Universal Database. The trace file for the update text

index function logs all errors regardless of the trace level that is set. When you update the text index, you can monitor the trace file for any errors and turn on more detailed tracing if needed. The library server system configuration parameter **UDFTRACELEVEL** contains the trace level setting.

The trace file name parameter, **UDFTRACEFILENAME**, contains the fully qualified path of the trace file name. For a library server on Windows, the default value of **UDFTRACEFILENAME** is *IBMCMROOT\log\ls\LSDBName\UDFTRACE*, where *LSDBName* is the library server database name. For a library server on UNIX, the default value of **UDFTRACEFILENAME** is *IBMWorkingDirectory/log/ls/LSDBName/UDFTRACE*, where *IBMWorkingDirectory* is the home directory of the system administration user that is defined during installation. For a library server on z/OS, the default value is *SYSPRINT*.

Finding problems by using DB2 Net Search Extender

Each indexing failure is recorded in the DB2 Text Information Extender event table for the index being updated. If the update of the text index was done manually, an error is returned and a message is placed into the server log with the name of the DB2 Text Information Extender event table that contains the error message. If the update of the text index was done automatically, then you must look at the DB2 Text Information Extender event table to determine if an error occurred. An entry is also written to the *icmplsud.log* for *ICMFetchContent* and *icmserver.fetchfilter* for *ICMFetchFilter*. Beginning with Version 8.4.2, entries are also written to the new trace file that is specified in the **UDFTRACEFILENAME** in the **ICMSTSYSCONTROL** system control table.

In most cases, the failed items are tried again the next time that the text index is updated. However, if the failure occurs the first time an index is updated, then they are not tried again automatically. DB2 Text Information Extender attempts to optimize performance for the initial loading of the text index, so it does not log failures for items that are tried again. However, it still logs the failure in the event table.

If a failure occurs on the initial update of one of the text indexes, you must take some actions or try to update the text index for these failed items. To prevent this extra action, you can load a small number of the items and then update the text indexes of these items instead of loading all of the items and performing an update on all of them. Because the first set of items is small, you have very few (if any) failures to retry. Retry any failures of future loads of the items, so that you do not need to retry them specifically. There is a performance penalty for loading only a small portion of the items at first because the initial update of the text index is faster than any subsequent updates.

If failures occur on the initial load, complete the following steps to find them and try them again:

1. Identify the index that you were updating and the DB2 Text Information Extender event table associated with it. To see the table name on which the text index was created and the table name that contains the index events:
 - a. Open a DB2 command prompt.
 - b. At the DB2 command prompt, issue the following query:

```
select tableschema,tablename,EVENTVIEWSCHEMA,EVENTVIEWNAME
from DB2EXT.TEXTCOLUMNS where indexname like '%TIE'
```

This query shows all of the text indexes for item types.

2. To find the failure, select from EVENTVIEWSHEMA.EVENTVIEWNAME as indicated in Step 1. This shows all of the errors that occurred when updating the text index.
3. The table also contains the primary key of the item that was not indexed. The primary key is in the PRIMARYKEY01 column of the table. The following query provides the primary keys and the messages:

```
select primarykey01,message from EVENTVIEWSHEMA.EVENTVIEWNAME
```

If the primary key is null, there was no error.

4. After you know which primary keys had failures, you can update each of the items so that they are tried the next time that the text index is updated. Use the following update statement:

```
update tableschema.tablename set tieref=tieref where  
compkey = pk01
```

where *tableschema.tablename* are the values selected above and *pk01* is the value of the primary key.

This process is required only once, for the initial failure. If fetching fails again, the failures are automatically tried.

Failures when the resource manager or Web server are down

When updating text indexes, if the resource manager or Web server are down and the library server cannot access the resource manager, the new and updated documents that are being processed will not be indexed.

Follow these steps:

1. Ensure that the resource manager and the Web server (if using port 80) are available.
2. If there is a need to re-index the whole item type again, follow these steps:

- a. Enter the following command, where *ItemTypeName* is your text searchable item type name:

```
SELECT t.componenttypeid from icmstnlkeywords k, icmsttextindexconf t,  
icmstcompdefs c  
where k.keywordclass = 2 and  
k.keywordname = ItemTypeName and  
c.itemtypeid = k.keywordcode and  
c.componenttypeid = t.componenttypeid;
```

- b. Enter the following command, where *xxxx* is the output from the previous step.

```
db2 update ICMUT0xxxx001 set TIEREF=TIEREF
```

Limitation: When you are using ICMfetchFilter or ICMfetchContent you cannot fetch objects from a replica resource manager when the main resource manager server is down.

Related information

ICMSTSysControl (System Control Table)

Logging and tracing for text search

Debugging items that are not indexed successfully

Text search with large objects:

The maximum file size of content that can be successfully full-text indexed is 60 MB. This means that you can successfully index large file sizes (for example, 100 MB) that have maximum of 60 MB of text.

Recommendation: If you are full-text indexing large documents on DB2 UDB, the value for the APLHEAPSZ might need to be increased. In a DB2 prompt, enter: DB2 UPDATE DB CFG FOR *databasename* USING APLHEAPSZ 7000, where *databasename* is the name of your database. You can increase the parameter higher than 7000 according to DB2 UDB recommendations. Otherwise, you might get a SQL0973N error indicating that not enough storage is available.

To enable this text search of objects larger than 25 MB, follow these steps:

1. Use the following script to increase the RETURNS CLOB for ICMFetchFilter to 20% of the largest non-text file to be indexed. In this example, 60 MB is used for the 20% calculated value:

```
drop function ICMFetchFilter;
create function ICMfetchFilter
(
    VARCHAR(512)
)
RETURNS CLOB(60M)
EXTERNAL NAME 'ICMNLUF!ICMfetch_Filter'
LANGUAGE C
PARAMETER STYLE DB2SQL
FENCED
READS SQL DATA;
```

2. While defining the item type, use the following table as a guideline for planning your text indexing strategy. Use the parameters below (Update Frequency, Commit Count) in the Text Search window for item type definitions:

Table 45. Parameters that you can use for item type definitions

File size	File type	Commit count (Number of files per index update)	Update frequency
300 MB	PDF, Word, Excel, 20% text	5	Every hour or less frequently
100 MB	text, 100% text	5	Every hour or less frequently

3. Depending on the size, number, or frequency, provide adequate machine resources to keep system from getting degraded. It is strongly recommended that you perform stress and endurance test with these large objects to arrive at an optimal set of resource requirements, before going into production.

Restriction: Documents exceeding the following file size might result in indexing failures:

- PDF documents above 150 MB
- Excel documents above 100 MB

Limiting the data that is extracted during text indexing:

If you want to limit the types of data that are extracted during text indexing, you can use the OITOPTIONFLAG system configuration parameter in the ICMSTSysControl system control table.

For most content management systems, the types of data that are extracted from objects such as documents during the text indexing process are sufficient for the users of the system. Beginning with Version 8.4.3, more types of data are extracted during text indexing than in earlier versions. For example, the text indexing technology extracts the text that is contained in an embedded object such as a diagram.

To limit the data that is extracted during text indexing:

Change the default values of the bits on the OITOPTIONFLAG system configuration parameter in the ICMSTSysControl system control table. See the system control table information for the definition of each bit.

Related reference

ICMSTSysControl (System Control Table)

Defining text search options for DB2 for z/OS

You can make attributes, resource items, and documents text-searchable from the system administration client.

To define text search options:

1. Click **Options** on the New Item Type Definition page or Attributes page to open the Text Search Options window.

Restriction: After you create the new text index, you can view the text search options on this window, but you cannot change these options.

Tip: If you open the Text Search Options window from the Attributes page, some of the fields described in this section are disabled.

2. If you want to use default values for all of the text search options, select **DEFAULT SYSTEM** in the **Copy settings from** field and click **Load**. Alternatively, select another entry from the list and click **Load** to copy that entry's values in the Text Search Options window.
3. Select the format to be indexed in the **Format** field. The IBM OmniFind Text Search Server for DB2 for z/OS requires the format or type of text documents (such as TEXT, HTML, XML, or INSO) that you intend to search. This information is needed when the documents are indexed. IBM Content Manager for z/OS supports the file formats that are supported by IBM OmniFind Text Search Server for DB2 for z/OS.
4. In the **CCSID** field, specify the supported code page (CCSID) that is used to create the text index. IBM Content Manager for z/OS supports the CCSID that is supported by IBM OmniFind Text Search Server for DB2 for z/OS.
All of the CCSIDs that are supported for conversion to UTF-8 by z/OS Unicode Conversion Services are supported by IBM OmniFind Text Search Server for DB2 for z/OS. For more information about z/OS Unicode Conversion Services, see *z/OS Support for Unicode: Using Unicode Services*. To display active conversions to UTF-8 on your system, use command **D UNI,CONV,TOID=1208**.
5. In the **Language code** field, specify the language code that is used to create the text index. IBM Content Manager for z/OS supports the language that is supported by IBM OmniFind Text Search Server for DB2 for z/OS.
6. In the **Index update settings** fields, specify parameters to control the frequency at which the index is updated. Specifically, you can specify the number of changes to the index before the next update, and the amount of time that passes before the update.

Text search index updates are not performed automatically. The scheduling of update requests is the responsibility of the DB2 for z/OS database administrator.

For **Update frequency**, select one of the following options:

Option	Description
Basic update frequency	Select to enter a simple numeric value and time period.
Advanced update frequency	Select to enter a string value that is supported by the text search engine. In the field, type five values, each separated by a space, as follows: <i>minute hour day_of_month month_of_year day_of_week</i>

For more information about how to specify the update frequency value, including the use of intervals and other advanced update frequency settings, see the IBM OmniFind Text Search Server for DB2 for z/OS documentation in the Information Management Software for z/OS Solutions Information Center.

Recommendation: Leave the **Commit count** field blank. Setting it to a nonzero value might lead to performance degradation. Before you commit a change to the database, the database records a log file of changes that can be undone. When you commit the update, this log file is erased, which makes your updates to the database permanent. You should not set a commit count to commit updates to the database. See the IBM OmniFind Text Search Server for DB2 for z/OS documentation for more information about this situation.

7. In the **User defined function name** field, select **ICMfetchContent** or type the name of your own user-defined function for fetching a document.

When you define text-searchable user attributes from the Attributes page, type the name of your own user-defined function. The user-defined function must return a value to DB2 for indexing. For example, you can pass the column or attribute value to the user-defined function for manipulation, then return the updated value to DB2 for indexing.

8. In the **User defined function schema** field, enter the name of the database schema in which the user-defined function is defined. If you use the standard user-defined function ICMfetchContent, you do not need to specify a user-defined function schema.

This field is disabled if you opened the Text Search Options window from the Attributes page.

9. In the **Update method** field, select one of the following options:


Option	Description
Update with backup	Select to index the documents on IBM OmniFind Text Search Server and then send the text index backup to DB2 for z/OS.
Update without backup	Select to index the documents on IBM OmniFind Text Search Server. The text index backup is not sent to DB2 for z/OS.

10. Click **OK** to save the information.

Related tasks

Optional: Configuring text search for DB2 for z/OS

Related information

 Information Management Software for z/OS Solutions Information Center

Updating the index for DB2 for z/OS:

IBM Content Manager includes a sample program that updates the index for you. You can also update the index manually.

The *IBM OmniFind Text Search Server for DB2 for z/OS Installation, Administration, and Reference Guide* provides more detailed information about how to update the index.

The IBM Content Manager sample program that updates the index automatically is called **S_{TextIndexUpdate}ICM**. There are Java and C++ versions of the program. The Java version has the file extension `.java` and the C++ version has the file extension `.cpp`. You can find the samples in the `IBMCMROOT\samples\` directory after you install the IBM Content Manager Version 8 Java and C++ connector toolkits on the workstation.

You can use **Index update settings** to set the frequency that the text index is updated during item type creation, and use the DB2 administrative scheduler to call the `SYSPROC.SYSTS_UPDATE` stored procedure according to a specific schedule based on the setting. However, there are times when items are in a queue waiting to be updated.

Use one of the following methods to immediately update the index:

- Issue the following **CALL** statement by using DB2 CLP (the DB2 command prompt) on your workstation after you connect the DB2 for z/OS subsystem.
- Run a stored procedure from QMF by issuing the following **CALL** statement from the SQL Query panel.

Tip: After you enter a **CALL** statement, a **RUN** command is issued to run the stored procedure.

- Run a program that calls the following **CALL** statement.

CALL statement:

```
CALL SYSPROC.SYSTS_UPDATE (indexSchema, indexName, options)
```

where:

- *indexSchema* identifies the schema of the text search index. If you are unsure of the index name, you can find out by entering the following query by using SPUFI or at a DB2 command prompt on your workstation: `select indexname, tablename from SYSIBMTS.SYSTEXTINDEXES`
- *indexName* identifies the name of the text search index.
- *options* is a character string that specifies the option that is available for this stored procedure. The available options are `USING UPDATE MINIMUM` or `ALLROWS`.

Related information

 Installing an IBM OmniFind Text Search Server for DB2 for z/OS

Correcting text indexing failures in DB2 for z/OS systems:

When an item type is made text searchable, the content for the document or resource items must be fetched from the resource manager for text indexing. The content is fetched when the text index is updated. When the text index is updated, failures can occur when the system fetches the contents from the resource manager. If a failure occurs on one item, the item is not indexed, but text indexing continues.

Finding problems in the UDFTRACEFILENAME trace file

Beginning with IBM Content Manager Version 8.4.2, the ICMSTSYSCONTROL system control table contains library server system configuration parameters for a trace file name and a trace level for the update text index function for the text search of objects on the DB2 Universal Database. The trace file for the update text index function logs all errors regardless of the trace level that is set. When you update the text index, you can monitor the trace file for any errors and turn on more detailed tracing if needed. The library server system configuration parameter **UDFTRACELEVEL** contains the trace level setting.

The trace file name parameter, **UDFTRACEFILENAME**, contains the trace file name. For a library server on z/OS, the default value of **UDFTRACEFILENAME** is **SYSPRINT**.

Finding problems by using the SYSIBMTS.EVENTS table

When the text index is updated, failures can occur when some of the contents are fetched from the resource manager. If a failure occurs on one item, the item is not indexed, but text indexing continues. Each failure is recorded in the table **SYSIBMTS.EVENTS_n**, where *n* is the index ID according to the **INDEXID** column of the **SYSIBMTS.SYSTEXTINDEXES** administration table for the index that is being updated. If individual documents contain errors, you must correct the errors and update the text search index again. You can look up the **ROWIDs** of the erroneous documents in the event table.

The failed items are tried again the next time that the text index is updated.

If there are failures, complete these steps to find them and try to index the items again:

1. Identify the index that you were updating and the event table that is associated with it. To see the table name for which the text index was created and the table name that contains the index events:

- a. Use **SPUFI** or open a **DB2** command prompt on your workstation.
- b. Issue the following query:

```
SELECT INDEXID, TABLESCHEMA, TABLENAME, EVENTTABLENAME
FROM SYSIBMTS.SYSTEXTINDEXES;
```

This query shows all of the text indexes for item types.

2. To find the messages, select * from **SYSIBMTS.EVENTS_{indexid}**, where the *indexid* is as indicated in Step 1.

Example: **SELECT * FROM SYSIBMTS.EVENTS₁₆₈**, where the *indexid* is 168.

This query shows all of the messages that occurred when the text index was updated.

3. The table also might contain the row ID of the item that was not indexed. The row ID is in the **RID** column of the table. The following query provides the **RID** and the messages:


```
SELECT HEX(RID),MESSAGE FROM SYSIBMTS.EVENTS_indexid WHERE RID IS NOT NULL
```

If the RID is null and the message does not state an error, there was no error.

4. For each row ID that has failures and is not null, you can update each of the items so that they will be indexed the next time that the text index is updated. Use the following update statement.

Remember: Skip this step if the row ID is null.

```
UPDATE tableschema.tablename SET TIEREF=TIEREF  
WHERE ROW_ID = ROWID(rid)
```

where *tableschema.tablename* are the values that were indicated Step 1, and *rid* is the value of the RID.

5. Call the SYSPROC.SYSTS_UPDATE stored procedure again. If the stored procedure returns successfully without any warnings, then all updated documents are included in the text search index.

Failures when the resource manager is down

When the text index is being updated, new and updated documents that are being processed cannot be indexed if the resource manager is down and the library server cannot access the resource manager.

Follow these steps:

1. Ensure that the resource manager is available.
2. If there is a need to re-index the whole item type again, invoke the following statement:

```
CALL SYSPROC.SYSTS_UPDATE (indexSchema, indexName, 'ALLROWS')
```

Limitation: When you are using ICMfetchContent, you cannot fetch objects from a replica resource manager when the main resource manager server is down.

Related tasks

Logging and tracing for text search

Related reference

ICMSTSysControl system control table

Related information

Debugging items that are not indexed successfully

Specifying CCSID for text search on DB2 for z/OS systems:

When you define the text search options, you can specify the coded character set identifier (CCSID) that is used to create the text index.

If you intend to index binary data or documents, you can specify the CCSID of the data. If any of the data is character data, DB2 recognizes the encoding and the CCSID specification is ignored.

All of the CCSIDs that are supported for conversion to UTF-8 by z/OS Unicode Conversion Services are supported by IBM OmniFind Text Search Server for DB2 for z/OS.

To display active conversions to UTF-8 on your system, use command **D UNI,CONV,TOID=1208**.

For more information about z/OS Unicode Conversion Services, see *z/OS Support for Unicode: Using Unicode Services*.

DB2 for z/OS text search with large objects:

The maximum document size is 100 MB. The IBM OmniFind Text Search Server for DB2 for z/OS limits the number of Unicode characters that can be indexed for each text document. Sometimes this character limit results in the truncation of large text documents in the text search index.

The default value for the number of Unicode characters that are allowed for each text document is 10 million. For a rich text document, this limit is applied after the document is transformed to plain text. This means that you can successfully index large file sizes, for example, 100 MB, that have a maximum of 10 million Unicode characters of text.

If a text document is truncated during the parsing stage, you receive a warning that some documents were not processed correctly or completely, and the document is partially indexed. Details about the warning are written to the event table that is created for the text search index. Text that is in the document after the limit is reached is not indexed and cannot be searched.

To enable this text search of objects that are larger than 25 MB, follow these steps:

1. Use the following SQLs to increase the RETURNS BLOB for ICMFETCHCONTENT to up to 100 MB:

```
DROP FUNCTION ?CREATOR?.ICMFETCHCONTENT          RESTRICT;

CREATE FUNCTION ?CREATOR?.ICMFETCHCONTENT
(
  VARCHAR(512)
)
RETURNS BLOB(25M)
COLLID ?DB2PKGCOLLID?
WLM ENVIRONMENT ?WLMENV?
PROGRAM TYPE SUB
EXTERNAL NAME ICMPLSUD
LANGUAGE C
PARAMETER STYLE DB2SQL
FENCED
STAY RESIDENT YES
READS SQL DATA NO EXTERNAL ACTION;
```

2. When you define the item type, use the following table as a guideline for planning your text indexing strategy. Use the following **Update Frequency** and **Commit Count** parameters in the Text Search window for item type definitions:

Table 46. Parameters that you can use for item type definitions

File size	File type	Commit count (Number of files per index update)	Update frequency
50 MB	PDF, Word, Excel, 20% (estimated) text	5	Every hour or less frequently
10 million Unicode characters of text	text, 100% text	5	Every hour or less frequently

3. Depending on the size, number, or frequency, provide adequate hardware resources to keep the system from becoming degraded.

Recommendation:

Perform stress and endurance tests with these large objects to determine an optimal set of resource requirements before you move into the production phase.

Defining text search options for Oracle

You can make attributes, resource items, and documents text-searchable from the system administration client.

To define text search options:

1. Click **Options** on the New Item Type Definition page or Attributes page to open the Text Search Options window.
2. If you want to use default values for all of the text search options, select **DEFAULT SYSTEM** in the **Copy settings from** field and click **Load**. Alternatively, select another entry from the list and click **Load** to copy that entry's values in the Text Search Options window.
3. Choose your index preferences:

Datastore

Specifies how your text is stored.

Filter

Specifies how documents are filtered for indexing. Your selection is based on your document formatting, character sets, and type. For example, HTML and plain text documents do not need filtering, so they can use the null filter option.

Lexer

Specifies the language of the text you are indexing.

Wordlist

Specifies the options you can set for query results.

Storage

Specifies how the index table should be stored.

Important: If you want to store the text index table in a user-defined table space, select the BASIC_STORAGE preference that you created for the user-defined table space.

Stop List

Specifies words not to index. The lists can include one language or multiple languages. You can create your own list, or you can modify the default list that comes with your database language.

Section Group

Specifies the area to index within a document.

4. Specify how the index will update:

Update every

Specifies the length of time between synchronization changes to the index.

Parallel degree

Specifies the degree to run parallel synchronization.

Maximum memory

Specifies the maximum runtime memory to use for synchronization. The more memory you allocate, the better the query performance.

5. Specify how the index will be optimized:

Update every

Specifies the length of time between optimizations, which will remove old information and can improve query time.

Parallel degree

Specifies the degree as a number for parallel optimization.

Maximum time

Specifies the maximum amount of time to spend on optimizing the index.

6. To specify additional options, enter the information in the **Option Name** field and corresponding **Option Value** field. Click **Add** to add the new option to the list.

For example, to set the runtime memory to use for indexing to 32 megabytes, add memory to the **Option Name** field and 32M to the **Option Value** field.

Refer to your Oracle documentation for a complete list of options available.

7. Click **OK** to save the information.

Restriction: Custom Lexer preference classes based on the MULTI_LEXER cannot be used in indexes on the content of document item types. The restriction is caused by the fact that the MULTI_LEXER requires that, for each data item, there is a column that includes the language code to use.

Related information

Planning custom table spaces for item type components and indexes to improve performance

Text search index update

If you use the ICMFetchFilter UDF, the system might hang or end abruptly when updating the text search index. When the system hangs and then ends abruptly, all of the documents that were not indexed before the abrupt end are not indexed by the system.

To ensure that your documents get indexed after a system hang or an abrupt end, enable the text indexing task to time out in the library server configuration window in the features page.

Locating an object that did not get indexed

When text indexing ends abruptly, the document that was being indexed does not get indexed, so you must locate and reindex that document.

To find the document, or object, complete the following steps:

1. In a DB2 command window, run the following command:

```
db2 "select EVENTVIEWSHEMA, EVENTVIEWNAME from
DB2EXT.TEXTINDEXES where INDSHEMA = 'ICMADMIN' and INDNAME =
'ICMUT01001001TIE'"
```

Where the text index name is ICMUT01001001TIE and the schema is ICMADMIN.

You receive a list of event views. Each event view has a column named MESSAGE. This column contains the message text corresponding to an error or SQL warning and SQL state that is returned by the ICMFetchFilter UDF.

2. Use the item ID and version ID to locate the document that did not get indexed in your system.

Example

Example SQL state warning returned by the UDF:

```
CTE0100 A DB2 operation failed. DB2 information: "01H20"  
"[IBM][CLI Driver][DB2/6000] SQL0462W Routine "ICMFETCHFILTER"  
(specific name "") has returned a warning SQLSTATE, with diagnostic  
text "A1001001A07G30B63645B75442 1 Timeout after 60 seconds".  
SQLSTATE=01H20
```

The first string is the item ID of the object that caused the system to stop, timeout. The next string is the object version ID. The 01H20 warning state means that a timeout has occurred. The diagnostic text is the text the UDF returned to NSE for this type of warning. Therefore, the example message indicates that an object with item ID A1001001A07G30B63645B75442 and version ID 1 timed out after 60 seconds.

Using the item ID and version ID, you can find the TIERef string associated with the document and invoke the UDF to test if the timeout value that was set is too small or if there is a problem with the object.

Before you invoke the UDF, disable the timeout feature by using the system administration client, or by running the following DB2 command:

```
db2 update ICMSTSYSCONTROL set UDFTIMEOUT=0
```

You can also set the value to a large number, such as 36000 seconds (again, using the system administration client or by issuing a DB2 command).

You can then manually invoke the UDF by entering the following command:

```
db2 "values icmfetchfilter('...')"
```

where ... is the TIEREF string from the previous step. The text data from the object should be returned.

Determining a text index timeout value

Determining what value to set for the text index timeout requires that you know the system well and that you do some testing of various values. When deciding what values to start testing, consider the following points:

- The resource manager needs time to retrieve documents from the resource manager database. Therefore, you should have an idea about the size of the objects you store and how long it might take to retrieve your largest object and how long it might take the resource manager to respond in your particular system topography.
- Because the system is flexible and you can set up a resource manager that is physically located far away from the library server, also take into consideration any possible network latency.
- Documents that have more text require more time from the system to extract the text. The system might also require more time to extract text from some file formats, such as PDF and Word.
- Documents that have a large amount of text require more time from the system to return the extracted text back to the library server.

Setting the value too small, such as one second, might cause a process to terminate before it has completed normal processing. Setting the value too large, such as one hour, does not affect performance in normal processing.

Exporting data as XML

You can select one or more objects and export them to a readable XML file or directly to another server. By exporting data as XML, you can transfer IBM Content Manager metadata, including data model objects, such as item types and their attributes, and administration objects, such as server definitions and access control lists, from one IBM Content Manager system to another.

You can export objects with their prerequisites. Each metadata object has a set of attributes. Some of these attributes might be other IBM Content Manager objects. These other objects are considered prerequisite, or dependent, objects.

Restriction: For a single export action, you cannot select objects of different types. For example, you cannot select to export some item types and some access control lists in the same export action. You can export these objects in two separate export actions.

Restriction: There are characters used for the name of a data model object for IBM Content Manager or IBM Information Integrator for Content that are not valid in the XML context. For example, XML does not allow "XML" to be at the beginning of an element or attribute name. Therefore, an item type name, "XMLDocument" cannot be directly mapped to an element name in XML. Another example is that the XML name does not allow spaces. Therefore, a federated entity named "project entity" cannot be exported directly as named in the XML element. The same rule applies to a federated attribute. To find a list of valid characters in XML, you can refer to the XML standard, <http://www.w3.org/TR/REC-xml#NT-Name>.

Exported files contain import statements that refer to IBM Content Manager schema files. These files are specific to your IBM Content Manager installation and are located in the `IBMCMROOT\config` directory. If you are using XML Services in IBM Content Manager administration, no action is necessary. If you want to load an exported file into a different tool, such as an XML editor, specify the location of `IBMCMROOT\config\cmdatamodel.xsd`. On Windows, the default location of `IBMCMROOT` is `C:\Program Files\IBM\db2cmv8`. On UNIX, it is `/opt/IBM/db2cmv8`.

To export data, complete the following steps:

1. In the navigation pane, select the object you want to export.
2. If you selected one or more container objects of the same type, right-click and select **Export to XML**. If you selected a single tree node, right-click and select **Export All to XML**. The Export Options window displays.
3. Under **Dependent definitions to also export**, select the appropriate check box to select any dependent objects that you want to export. For example, if you are exporting an item type, it might have a dependency on an access control list or an attribute group. So for this example, you can select the check boxes for **Data model definitions** or **Administrative definitions**.
4. Under **Export destination**, you can export your metadata to a file or to another server:

Option	Description
To file	<p>Export your data directly to a file.</p> <ol style="list-style-type: none"> 1. Browse to the directory you want to store the file. 2. Enter a file name. <p>The file containing data model objects has a file extension of .xsd. A file containing administrative objects has an extension of .xml.</p> <p>You can import the file after it is created to another system using the Tools > Import XML command.</p> <p>Note: Importing an XML file to create an item type, even with a successful action, might result in one of the following error messages being displayed in the DK log file:</p> <ul style="list-style-type: none"> • DGL0690A: No matching method and parameters. • DGL3898A: Component type ID does not exit. <p>The error messages in this case are the result of the logical flow of creating an item type and component type object that has not yet been added to the database. Therefore, these error messages can be ignored.</p>
Directly to another server	<p>Export your data directly to another server that is defined to the system administration client.</p> <ol style="list-style-type: none"> 1. Select the server name from the list. 2. Select your export preference: <ul style="list-style-type: none"> • To watch the export progress and see the results, select Process interactively. • To let the process run in the background and view the results in a log file, choose Process in background and log results. If an error occurs it is logged, and processing continues with the next object.

5. Click **OK** to export the selected objects. The Export Progress window displays, showing the status of your action.

To properly import a particular object, all of the prerequisite objects have to either exist or be already imported to the system. To guarantee that this action occurs, the export order is important. When you choose to export an object with the prerequisite option on, the proper order is ensured. However, IBM Content Manager cannot handle the situation where there is a cyclic dependency among objects of the same type.

For example, there are three item types: A, B and C. Here is how they are related to each other:

- Item Type A depends on Item Type B (because of a foreign key definition)

- Item Type B depends on Item Type C (because of an auto foldering definition)
- Item Type C depends on Item Type A (because of a foreign key definition)

A warning message is logged in the connector log file and is displayed in the system administration client when this situation is detected during XML export. The message in the log file describes where the cycle is. In the example, the following log message is found in the log file: [MSG]: There is a cycle ([A, B, C]) within the dependent objects of A of type ITEM TYPE. When import the definitions to another system, please remove the cycle before import the XML document.

To work around this problem, complete the following steps:

1. Make a copy of the exported XML file.
2. Break the cycle in the XML file. In the example, remove the foreign key definition temporarily from C to A in the XML export file.
3. Import the modified XML file.
4. Add the removed definition back to the XML file. In the example, it is the foreign key definition from C to A.
5. Import only the objects being affected. In the example, it is the item type C.

During the export process, the real password of a system administration object, such as a user, is not exported. The default text password is used instead. This feature is introduced for security reasons. There should not be any real password in clear text written in the export file.

The following system administration object passwords are exported as password:

- password for user
- password in the resource manager server definition (CMResourceManagerDefinitions)
- resource manager password in the resource manager configuration definition
- DB2 Text Information Extender or DB2 Net Search Extender password for the library server configuration

When the export process is finished, each of these objects has password as the password.

If you want to import the exported object back to the database, change the default password in the exported file before importing it. Otherwise, the default password (password) is imported into the target system. This rule applies to all the system administration objects that have password fields.

Because the exported password is always the default text password, while importing in interactive mode, the comparison is based on the target system having the default password also. Even though the passwords in the source object and target system object are the same, the conflict might still arise.

Exporting item types to a WSDL file

You can export your item types into Web Services Description Language (WSDL) files.

IBM Content Manager provides a self-contained, self-describing modular interface, called a Web services interface, that you can use within your applications, with other Web services interfaces, or in complex business processes to seamlessly

access items stored in an IBM Content Manager system. A Web service interface is a reusable, loosely coupled, software component that can be located, published and invoked through a network, like the Web. The Web services model leverages the WSDL and other technologies and protocols to provide an environment that makes application integration easier, faster, and more cost effective.

To export your item type to a WSDL file, use these steps:

1. From the System Administration Client window, right-click an item type and select **Export to WSDL file** to open the Save WSDL File As window.
2. Browse to the directory you want to store the file.
3. Enter the name of the file.
4. Click **Save**.

For more information about WSDL files and Web services, see the *Application Programming Guide*.

Importing data

You can import one or more data model objects, like attributes, attribute groups, or item types, or system administration objects, like users, privileges, and access control lists, from a readable XML file. You can also use this feature in conjunction with the **Export** menu to move metadata objects from one system to another.

Restriction: There are characters used for the name of a data model object for IBM Content Manager or IBM Information Integrator for Content that are not valid in the XML context. For example, XML does not allow "XML" to be at the beginning of an element or attribute name. Therefore, an item type name, "XMLDocument" cannot be directly mapped to an element name in XML. Another example is that XML name does not allow space. Therefore, a federated entity named project entity cannot be exported directly as named in the XML element. The same rule applies to a federated attribute. To find a list of valid character in XML, you can refer to the XML standard, <http://www.w3.org/TR/REC-xml#NT-Name>.

To import data from a readable XML file:

1. From the main menu, click **Tools > Import XML**. The Import XML Options window displays.
2. Click **Browse** to select the file from which you want to import the objects, either an .xsd file for data model objects or an .xml file for administrative objects.
3. Select your import preference:
 - To watch the progress and see the results, select **Process interactively**.
 - To run the process in the background and view the results in a log file, choose **Log results to XML import log**. If an error occurs, it will be logged and the processing will continue with the next object.
4. Click **Import** to begin the import process.

If you receive DGL0683A: Internal error: The root element required 'CMResourceManagerDefinitions' is not unique in the source system or file or DGL0683A: Internal error: The root element required 'CMSysAdminDefinitions' is not unique in the source system or file, you might be attempting to import to the incorrect server type.

For example, if you received the first error message, you have a resource manager selected but the import file contains library server definitions. To avoid these errors, select the appropriate server name, then select **Tools > Import XML**.

If you receive the second error message, you might be trying to import IBM Content Manager objects that are not supported for XML import. The following types of IBM Information Integrator for Content objects are supported for XML import:

- Server configuration
- Federated entity
- Search template

Importing data from XML

When you export interactively to another server, or import interactively, the Import Preprocessor Results window displays your interim results so that you can take appropriate action before proceeding. This window also appears when you are importing from an XML file that you exported to a file.

Attention: When performing an XML import with the Process Interactively option, the Import Preprocessor Results window might indicate that some of the objects to be imported have conflicting definitions. These conflicts are shown graphically by the **Different** or **New different** icons. The **Different** icon means that one or more of the properties of an existing object is different from the properties in the import file. The **New different** icon means that the object does not yet exist and that one or more of the properties in the import file has been modified automatically. Both the **Different** and **New different** icons are intended to alert you to a change, possibly not expected, to either the system or the import data. Neither indicates that the import will fail. Conversely, not having one of these icons is not an indication that the import will succeed.

The import results depend on the objects that reside on the target system and the objects that you are trying to import. There are three possible scenarios:

Target system is empty

You can successfully create the objects in the target system because all of the objects being imported are new. This scenario is common when you are importing to a new system.

Target system has non-conflicting objects





You can successfully create the objects in the target system.

Target system has conflicting objects

You must decide whether to update the objects on the target system with the objects from the import file or to change the import objects to fit the target objects. This scenario can include the case where a new object cannot be imported without modifying one or more properties.


Each object that you have selected to import is displayed under its entity name, for example, Users, Attributes, or Item types. You can expand the results tree to see all of the objects. Each object has an icon next to it, representing the state of the object in the source and target systems.

Table 47. Icons showing the state of the object

Icon	State
	New. The object does not exist on the target system and can be imported without modification.
	New Different. The object does not exist on the target system, but one or more properties of the object must be modified before import.
	Equal. The object already exists on the target system, but its definition matches that of the source entity. This comparison considers the definition of the entity itself, not any other entities it might reference.
	Different. The object already exists on the target system and at least one property of the source is different from that property on the target system.

To continue the import process:

1. Review the icons next to each object to determine their import state. The new and equal objects are already in the import state and they will be imported when you click **Continue**.
2. Right-click each different object and select one of the following commands:

Command	Select this option to
View details	Open the Details of Import Definition and Target Definition window so that you can see the differences between the source and target objects.
Import	Toggles between the Do Not Import state and the previous state of the object. You must indicate what you want the system to do for the objects that are listed as different.
Do Not import	Delete the object from the list of objects that you are importing.  The object will not be imported when you click Continue .




3. Click **Continue** to open the Import Confirmation window. **Continue** is enabled only if there are no objects still in the new different state or different state, and at least one object to import.

Attention: During the import process, if there is a new data model object imported, such as an item type or attribute, the Import Preprocessor Results window shows this data model object with a conflict. When the Details of Import Definition and Target Definition window is open, the conflict normally is shown by the description field. The source and target of the description field have the same value, and the state for this description field is marked as equal. This data model object conflict can be confusing because no such object exists in the target system yet. You should simply ignore the conflict mark, click the Accept button, and continue importing. The displayed conflict does not prevent the import.

Resolving import conflicts

When you choose to view the details of the import action for an object, the Details of Import Definition and Target Definition window displays. This window shows the difference between the source and target objects. Use this window to confirm your import results before proceeding.

1. **Optional:** Select **Show All** to display all of the objects you are importing. The default, **Only show properties that have differences**, reduces the displayed objects to only those objects with differences between the source and target systems.
2. Review the displayed information to verify that you are importing what you expect:

Option	Description
Icon	 <p>New. The property does not exist on the target system. The value of the Source column will import unless you make a change.</p>  <p>Equal. The Source, Existing target, and Resulting target values are identical.</p>  <p>Different. The value for this property is different from that on the target system.</p>
Properties	Displays the names of each of the entities properties
Source	Contains the value of each property from the import file
Existing target	Contains the value of the property as currently defined in the target system. If the property does not exist in the target system, the entry is empty.
Resulting target	Contains the value that will import.

3. **Optional:** Edit the Import Results column to select a different value for the imported property for the object. If a value already exists on the target system, the object must be able to be updated. Otherwise, the value on the target system remains. The following list contains the properties that you can modify:

Entity name	Property name
library server configurations	library ACL name
users	default resource manager
users	default SMS collection
users	user ACL
item types	access control list
item types	resource manager
item types	collection
item types	prefetch collection
work nodes	access control list

Entity name	Property name
work nodes	folder item type
work nodes	required item type
processes	access control list
worklists	access control list

- Click **Accept** to confirm you want to import the object and save any changes you might have made.

Import selection confirmation

After you choose the files to import into your target system in the Import Preprocessor Results window, you can choose how you want to handle any errors during the import process.

From the Confirm Import Selection window, you can review the list of objects that you selected to import and decide how to proceed.

- Choose whether to continue importing the objects if an error occurs:

Option	Description
Log error and abort	If an error occurs, the system adds the error to a log file and cancels the import action.
Log error and continue	If an error occurs, the system adds the error to a log file and continues importing objects.

- Select how you want to proceed:

Option	Select this button to
Import	Begin the import process.
Save	Save the selections that you made, including which objects to import and properties you have modified, to a file so you can import later. The Save Import File As window displays, from which you can select the directory and specify a file name.
Cancel	Closes the window without saving your information.

Mapping and importing XML schemas into IBM Content Manager

The XML schema mapping tool enables you to convert an XML schema file (.xsd) into another XML schema that you can import as an IBM Content Manager item type. The source schema can be automatically transformed into a default storage schema. You can edit the structure and some properties of the storage schema using the XML schema mapping tool before you import it into IBM Content Manager. In addition, you can export an existing IBM Content Manager item type as a storage schema and directly enter a mapping between a source schema and the item type. Use of the XML Schema Mapping tool results in the automatic creation of an additional item type and set of attributes. These objects will display with other similar objects in the system administration client.

Restrictions:

- DTD schemas are not supported. There are many programs available to convert DTDs into XML schemas.
- Annotation support is not complete in DB2 Content Manager Version 8 Release 3 of the XML schema mapping tool. When a target schema is loaded, some annotations will be lost, and none will be preserved when saving a mapping.
- Although the XML schema mapping tool allows you to create a document item type, you must use the system administration client to add parts to the item type.

The XML schema mapping tool keeps the mapping between the source and storage schema and creates an XSLT script that you can use later to transform XML documents that conform to the source schema into documents that conform to the storage schema. You can import these transformed XML documents into IBM Content Manager as items. The XML schema mapping tool uses the working IBM Content Manager server as persistent storage, enabling you to save and share your XML mappings.

To start the XML schema mapping tool:

Windows

Restriction: To run the XML schema mapping tool, a user must have the appropriate permissions to create and modify files in the *IBMCMROOT\admin\common* directory. If it is not possible to permit this access for a user account, you can modify the shortcut that starts the XML schema mapping tool so that it starts in a different directory. Open the shortcut's properties and change the **Start in** field to a directory that the user has appropriate access to.

To start the XML schema mapping tool, click **Start > Programs > IBM Content Manager Enterprise Edition > XML schema mapping tool**.

UNIX

1. At the console, change to a subdirectory for which you have appropriate permissions to create and modify files, such as your home directory.
2. Execute the following command to start the XML schema mapping tool:

```
IBMCMROOT/admin/common/cmxmlmap81.sh
```

Creating an XML schema file

The process to create an input XML schema file from an existing XML schema file (.xsd) consists of the following tasks:

1. Creating a mapping
2. Selecting a source schema
3. Generating the storage schema

Each of these tasks is described in detail below.

Creating a mapping

To create a mapping, follow these steps:

1. Select **Mapping > New** from the main menu or click the new mapping button on the toolbar. The tool creates a new, empty map and displays it in the mapping pane. The default name for this new mapping is `New_Mapping1`.
2. Rename the new mapping to something meaningful by clicking **New_Mapping1** to select it, then right-clicking and selecting **Rename**. The Rename Mapping window displays.
3. Enter a new name and click **OK**.

Selecting a user schema

Next, you select the XML schema to convert into a storage schema.

1. In the mapping pane, click **Source Schema** to select it, then right-click.
2. Click **Add from file system**. You can browse to the XSD file that you want to use. Any included or imported file from this schema is also loaded automatically.

The XML mapping tool requires one root element be identified for each schema loaded. If you have more than one root XML elements for a schema, you are prompted to select the name of the root element that you want to use from the Multiple Roots Detected window.

The schema file name is added under **Source Schema** in the mapping pane, and the loaded schema appears in the source schema pane.

There are many icons used in the source schema mapping pane to indicate different conditions. The following list provides an explanation of the icons.

Table 48. Source schema icons













Icon	Description
	An attribute belonging to a parent element. The attribute is required.
	An attribute belonging to a parent element. The attribute is optional.
	A root element that does not allow content. The element is required. The element is probably of complex type.
	A root element that does not allow content. The element is optional. The element is probably of complex type.
	An element that allows content. The element is required. If this is a leaf-level element, a simple type name accompanies the element name. If it is not a leaf-level element, it allows mixed content and has a complex type.
	An element that allows content. The element is optional. If this is a leaf-level element, a simple type name accompanies the element name. If it is not a leaf-level element, it allows mixed content and has a complex type.
	An element that does not allow content. The element is required and might repeat many times.
	An element that allows content. The element is optional and might repeat many times.
	An element that does not allow content. The element is required and might repeat many times.

Table 48. Source schema icons (continued)

Icon	Description
	An element that allows content. The element is required and might repeat many times.
	The complex type uses a sequence model group. This icon represents a repeating element (one or more times).
	This complex type uses an all model group.

Generating the storage schema

To generate a storage schema from a given loaded source schema, follow these steps:

1. In the mapping pane, click **Target Schema** to select it, then right-click.
2. Select **Generate from Source Schema**.

The XML mapping tool analyzes the structure of the source schema and makes the necessary changes to create a valid storage schema. For example, all leaf-level elements are converted into XML schema attributes, string types are converted into variable length strings, and choice model groups are changed to sequences.

The tool keeps track of where each element and attribute in the source schema ends up in the storage schema. These correspondences display as lines across the two panes.

Highlighting indicates that a change occurred to that element name or type during the conversion. In addition to the highlighting, changed element names are shown in blue so they can be distinguished from type changes.

Important: Before the target schema can be a valid IBM Content Manager storage schema, you must compare the element and attribute names to existing names in the IBM Content Manager server where you want to deploy the schema. To do this, you must validate the schema, which requires you to connect to the IBM Content Manager server first. See “Validating a storage schema” for more information.

Validating a storage schema

Target XML schemas must be validated before you can import them as an item type. The validation process transforms the current target schema into a potential storage schema. You can validate a schema at any time. Validation is also automatically invoked when you generate the storage schema based on the source schema, and when the storage schema is about to be imported.

To validate a storage schema, follow these steps:

1. Select the target schema under **Target Schema** in the mapping pane.
2. Right-click, then select **Validate as Storage Schema**. The tool checks to see if you are connected to an IBM Content Manager server. If you are not connected to a server, you are prompted for a database name, user ID, and password.

There are two types of validation, depending on whether the tool is connected to the IBM Content Manager server where the storage schema is being deployed:

Local validation

If the tool is not connected to an IBM Content Manager server, it cannot verify whether the target schema names are already used as component names in the IBM Content Manager server. It cannot verify that attribute names already exist in the IBM Content Manager server. The tool simply checks for potential name conflicts within the target schema. The produced storage schema is not guaranteed to import successfully because of the potential name conflicts at the IBM Content Manager server.

Global validation

If the tool is connected to an IBM Content Manager server, it checks the storage schema's element and attribute name with the already existing names of item types, components, and IBM Content Manager attributes. Any element that can cause a conflict is renamed in the tool's storage schema. Notice, however, that this still does not guarantee that the produced storage schema can be imported without any conflicts. There is always the chance that some other user will create a conflicting IBM Content Manager type or attribute on the server between the time you complete the validation and the time you attempt to import the storage schema.

Validation changes

Validation can change the shape and data types of the storage schema. Here is a list of the typical changes that occur:

Renaming

XML schema elements and attributes are renamed if a potential name conflict is detected. Every element and attribute name is compared against a set of names already in use. Names in this set come from two sources:

- The names in the schema themselves. Because the names in the schema are going to be imported as item types, components, and attributes in the IBM Content Manager server, conflicts can occur with the name within the schema. These are the only names used for renaming if the tool is not connected to the IBM Content Manager server when validating.
- The names of existing item types, components, and attributes on the connected IBM Content Manager server.

There are different renaming rules depending on the type of schema element under consideration.

XML elements names

Element names become IBM Content Manager component types when imported. The names of XML elements are compared with existing components (if connected) and the names of other elements in the schema.

XML attribute names

XML attribute names become IBM Content Manager attributes. XML attribute names conflict if an existing attribute has the same name and the attributes have different data types. For example, two attributes named ID will conflict if one has an integer data type and the other is a string. On the other hand, if two attributes are named ID and both are integers, then there is no conflict (both refer to the same global attribute).

Root XML element

The root element name becomes the name of the item type. This name is compared with existing item type names and renamed if needed. This check occurs only if the tool is connected to an IBM Content Manager server.

Primitive data types can be replaced

IBM Content Manager attributes cannot handle all XML data types. The tool converts and casts some primitive data types into data types that can be directly handled by IBM Content Manager attributes. The following table displays some examples of common conversions.

Table 49. XML data type conversions

XML data type	Converts to this data type
int, long, negativeInteger, nonNegativeInteger, nonPositiveInteger, positiveInteger, unsignedInt, unsignedLong, positiveInteger	integer
string	string, with some restrictions (a <i>maxLength</i> , for example). This restriction is then interpreted by the import libraries as a <i>varchar</i> with the given <i>maxLength</i>
anyURI, boolean, duration, ENTITY, gDay, gMonth, gMonthDay, gYear, gYearMonth, ID, IDREF, language, Name, NCName, NMTOKEN, NOTATION, QName, token	string, with <i>maxLength</i> set to the default maximum length.
ENTITIES, IDREFS, NMTOKENS	string, with <i>minLength</i> = 1 and <i>maxLength</i> set to the default maximum length.
byte, unsignedByte	short
hexBinary	base64Binary

Leaf-level elements become attributes

All leaf-level elements of the source schema become attributes in the target schema. XML documents allow values to be stored as either content of an element or as attributes of an element. In IBM Content Manager, values are stored only as attributes.

New attributes to hold content

This is a side-effect of the leaf-level element. Because only IBM Content Manager attributes can hold values, new attributes are created in the target schema to hold the content of non-leaf XML elements that allow mixed-content. In general, these new elements have the suffix `_text`.

Restructuring

The source schema is restructured when it is converted into a storage schema:

Table 50. Source schema converted to storage schema

Source schema	Storage schema
all or choice model groups	Converted to sequence. Choice, in particular, is not supported in storage schemas.
Nested groupings of sequence model groups	These are collapsed to one top-level sequence with the correct cardinality (minOccur, maxOccur) preserved

Table 50. Source schema converted to storage schema (continued)

Source schema	Storage schema
key, unique, keyref	These definitions are not supported in storage schemas. They are removed when validated.
attribute groups	References are replaced by the set of attributes in the group.

Importing a storage schema

To import the storage schema into IBM Content Manager as an item type, follow these steps:

1. Select the target schema under **Target Schema** in the mapping pane.
2. Right-click, then select **Import as Content Manager Item Type**.

If any changes occurred since the last validation, the tool validates the schema again then sends it to the XML services API for inclusion in the IBM Content Manager server as an item type.

No further changes are allowed to the storage schema, which is now marked read-only.

Creating a query

The XML schema mapping tool keeps the mapping between the source and storage schema and creates an XSLT script that you can use later. This XSLT script is the result of creating a query.

To create a query, follow these steps:

1. After you have created a correspondence between the source and target schemas and validated it, right-click **Query** and click **Refresh Query**. An XSLT script is created and added to the mapping.
2. **Optional:** You can update the XSLT script anytime after changing the mapping by selecting **Refresh Query**.

Saving your mapping

You can save a mapping session into the XML schema mapping tool repository, an IBM Content Manager repository that is created the first time a mapping is saved to an IBM Content Manager server. You must have a connection to an IBM Content Manager server to save your mapping.

To save the current mapping, follow these steps:

1. Click **Save Map** from the toolbar, or click **Mapping > Save**.
2. **Optional:** If you are not connected to an IBM Content Manager server, you are prompted for the database name, user ID, and password.
3. **Optional:** If you have not given a name to your mapping, you are prompted to rename it.

You can click **Mapping > Open** to retrieve stored mappings from the tool repository.

XML schema mapping tool interface

When you open the tool, you see three main sections or panes, from left to right: the mapping navigator, the user schema viewer, and the storage schema viewer/editor.

Table 51. The XML schema mapping tool panes

Pane name	Pane function
Mapping pane	Displays the current state of the mapping. A mapping is composed of the following parts: <ul style="list-style-type: none">• Mapping name• Source schema• Target schema• A list of correspondences between the source and target schemas• The queries generated by the correspondences
Source schema	Displays the user XML schema elements and attributes in tree form.
Target schema	Displays the storage XML schema elements and attributes, and enables you to modify the structure and properties of the storage schema.

Each of these panes have their own functions available by right-clicking various elements. The following sections describes these functions in detail.

Mapping pane

The mapping pane displays information about the current mapping session.

Table 52. Mapping pane commands

Display name	Right-click command	Description
Mapping name	Rename	Renames the mapping session with a new name you specify.
Source schema	Add from file system	Loads source schema from an XML schema (.xsd) file from your local file system. If the XML schema contains multiple root elements, you must select the one root element from the list to load. The name of the loaded file displays as a child of the source schema element. Restriction: DTD schemas are not supported. There are many programs available to convert DTDs into XML schemas.
Source schema	Remove schema	Removes a source schema from the mapping session.

Table 52. Mapping pane commands (continued)

Display name	Right-click command	Description
Target schema	Add from file system	<p>Loads target schema from an XML Schema (.xsd) file from your local file system.</p> <p>If the XML schema contains multiple root elements, you must select the one root element from the list to load. The name of the loaded file displays as a child of the target schema element in the mapping pane.</p> <p>Restriction: DTD schemas are not supported. There are many programs available to convert DTDs into XML schemas.</p>
Target schema	Export a Content Manager item type	<p>Loads an existing IBM Content Manager item type as the tool's target schema. This action requires the mapping tool be connected to the IBM Content Manager server where the item type resides. If it is not currently connected, the tool prompts you for a database, user name, and password for the connection.</p> <p>After it is connected, the tool displays the names of all available item types from the IBM Content Manager server. Select one item type to export as a target XML schema.</p> <p>Because this target schema represents an existing item type, the target schema will be read-only and cannot be modified using the schema editor nor imported as a storage schema.</p> <p>Restriction: There are characters that can be used for names of data modeling objects in IBM Content Manager that are not valid in the XML context. For example, XML does not allow the character string "XML" to be used at the beginning of an element or attribute name. Therefore, an item type named "XMLDocument" cannot be directly mapped to an element name in XML, and thus cannot be exported as a target schema in the XML schema mapping tool. To find a list of valid characters in XML, see the XML standard, http://www.w3.org/TR/REC-xml#NT-Name.</p>

Table 52. Mapping pane commands (continued)

Display name	Right-click command	Description
Target schema	Generate from source schema	<p>Converts the schema in the source schema pane into a storage schema. The conversion changes some XML schema elements into XML schema attributes, renames some of the elements, and changes some of the data types.</p> <p>The conversion attempts to validate the created storage schema if the tool is connected to the target IBM Content Manager server.</p> <ul style="list-style-type: none"> • If the tool is not connected, the resulting storage schema is partially validated. That is, potential name conflicts that are detected by reviewing the names mentioned in the schema itself are resolved. Partial validation does not check the names against elements in the target IBM Content Manager server. • If the tool is connected, the resulting storage schema is fully validated. Potential conflict names with item types, components, and attributes in the connected IBM Content Manager server are detected and fixed. (See “Validating a storage schema” on page 228 for more details.) <p>Because the resulting target schema was generated based on the current source schema, all possible correspondences among the two schemas are generated automatically. These correspondences display as lines across the two schema panes and are displayed under the Correspondences tree of the current mapping session in the mapping pane.</p> <p>You can modify the target schema using the schema editor, remove the generated correspondences using the Correspondence > Delete command, or add new correspondences using the Correspondence > Add command.</p>
Target schema	Remove schema	Removes a target schema from the mapping session.
Target schema	Save to file system	Saves the current target schema into a file. You can inspect the resulting XML schema file with an XML viewer or use the file with other IBM Content Manager tools.
Target schema	Validate as storage schema	See “Validating a storage schema” on page 228.

Table 52. Mapping pane commands (continued)

Display name	Right-click command	Description
Target schema	Import as Content Manager item type	<p>Imports the schema into an IBM Content Manager server as an item type. The tool runs a final validation on the schema if the mapping session has changes since the last validation. A connection to an IBM Content Manager server is required.</p> <p>If the tool is not connected, you are prompted for a database name, a user name, and a password.</p> <p>After connection, the current IBM Content Manager item type names from the IBM Content Manager server are displayed in a list for you to select. Enter the name to use for the new item type (the root element name is suggested by default) and click OK. The storage schema is then imported into IBM Content Manager as an item type.</p> <p>If successful, the target schema pane becomes a schema viewer and no further edits to the schema are allowed (the schema is now read-only).</p>
Correspondences		<p>Correspondences between the source and target schema are depicted using the xpaths of the schema elements involved in the correspondence. For example, the correspondence for an element called state is represented in the correspondence list as follows:</p> <pre>/statistics/cityStat/organization/addr/state-> /statistics/cityStat/organization/addr/@state</pre> <p>This correspondence is read as follows: The value of the state element of addr (under /statistics/cityStat/organization) is mapped into the value of the state attribute under the addr element of the target schema.</p>
Query		<p>Displays a list of query terms that together make up the query that implements the current mapping. The list represents the XSLT query scripts that implement the mapping.</p> <p>This representation is for illustration purposes only. You cannot add, delete, or edit the query component from the representation. You can, however, see and execute the queries by right-clicking on the query and clicking the appropriate command.</p>
Query	Refresh Query	<p>Updates the query. The query element is not updated automatically when there is a change in the mapping session, except in the following two cases:</p> <ul style="list-style-type: none"> • When you save mappings into the mapping repository, a new query is computed and saved into the mapping. • When you load a mapping from the repository, the query in the loaded mapping is computed when the mapping is loaded.

Table 52. Mapping pane commands (continued)

Display name	Right-click command	Description
Query	Open XSLT	Opens a window that displays the XSLT scripts that implement the current mapping query. The computed query is composed of two scripts. The window shows the boundary between the two scripts. This command does not automatically refresh the query before executing this action.
Query	Save XSLT	Saves the XSLT scripts that implement the current mapping into a file. This command does not automatically refresh the query before executing this action.
Query	Run XSLT	<p>Executes the created XSLT scripts.</p> <p>The script is divided into two scripts that are executed one after another, with the output of the first script used as input to the second script.</p> <p>You select the input XML document to be transformed by the query. The tool assumes the input XML document conforms to the source schema and does not run a separate validation of the XML document against the source schema.</p> <p>Similarly, the resulting XML document is not validated against the target schema.</p> <p>You can copy and paste the resulting XML document into the editor of your choice.</p> <p>This command does not automatically refresh the query before executing this action.</p>

The menus across the top of the tool enable you to create and work with your mappings:

Mapping menu

- New** Creates a mapping session. The new mapping will have a generic name and includes no source or target schemas.
- Open** Opens a previously saved mapping session from the mapping repository in the IBM Content Manager server. A connection to that server is required. To change the current connection, use the **Repository** menu.
You can select the session to open from the list that IBM Content Manager displays.
- Save and Save As**
Saves the current mapping session into the mapping repository.
- Close** Closes the current mapping session but not the tool. If there are unsaved changes in the current session, you are prompted to save the current mapping, discard the changes, or cancel the close operation.

Properties

Opens the Properties window in which you can change the default maximum string length and select two options for improved accessibility:

- Use system colors rather than standard mapping tool colors so that system display color settings will be used.
- Enable adding source elements to an existing mapping, which is easier for keyboard users, rather than having to specify them all at once.

If you change a property, you can save the change in the properties file so it is effect each time you start the mapping tool.

Exit Closes the mapping tool. If there are unsaved changes in the current session, you will be prompted to save the current mapping, discard the changes, or cancel the exit operation.

Repository menu

Connect

Connects the mapping tool to an existing IBM Content Manager server. The Connection window prompts you for a database name, user name, and valid password and creates the connection. If the connection is successful, the connection name is displayed in the lower-right corner (in the status bar) of the mapping tool.

Attention: The new connection replaces any existing connection without further warning unless you click **Cancel** on the Connection window.

Disconnect

Disconnects the mapping tool from the server. When disconnected, a No Connection message appears in the lower-right corner of the mapping tool.

Delete Mapping

Removes a previously saved mapping from the mapping repository. A connection to the IBM Content Manager server containing the mapping is required. IBM Content Manager prompts you to select the name of the mapping session or sessions to delete.

This command has no effect on the current mapping session.

Correspondence menu

Add Creates a new correspondence between one or more elements of the source schema and one element of the target schema. One or more valid source elements and one valid target element must be selected from the source and target schema panes to use this command. A gray dotted line appears between the schemas if a correspondence can be created between the selected elements.

In general, valid schema elements for correspondences are all leaf-level elements and elements that can hold a value. Target elements should not already have a correspondence to them.

After the dotted line displays, you can click **Correspondence > Add** to create the correspondence. The correspondence displays as

a solid blue line between the elements, and also appears in the list of correspondences for the current mapping session in the mapping pane.

Delete Removes an existing correspondence from the current mapping. You must first select a correspondence by doing one of the following actions:

- Select a target element that already has a correspondence to it. The blue line displays between the source and target panes.
- Open the Correspondence list for the current mapping in the mapping pane, then select the correspondence from the list. The selected correspondence displays as a blue line between the source and target panes.

After the correspondence is selected, you can click **Correspondence > Delete** to remove the correspondence.

Edit XSLT Expression

Use this menu item to enter a user-defined transformation function for a correspondence. For example, you might want to concatenate two fields from the source schema into one field of the target schema. To use this operation, you must first select an existing correspondence.

After the correspondence is selected, select **Correspondence > Edit XSLT Expression** to open the Edit XSLT Expression window. You can use the editor to edit an existing XSLT function using the source xpaths as input parameters.

Using the Content Manager for z/OS high-volume batch load utility

You must customize the sample high-volume batch load job, and you must generate the load program again when specific conditions occur. It is important to understand the supported functions of the high-volume batch load utility for the Content Manager for z/OS before you customize the sample jobs.

You can use the high-volume batch load utility to efficiently load large quantities of data into the Content Manager for z/OS library server and into the OAM that the z/OS resource manager uses to manage the storage and retrieval of objects in the same LPAR.

Tip: You can use the Content Manager for z/OS Job Configuration tool to configure jobs for the high-volume batch load utility.

You must complete two stages of configuration before running the batch load utility:

1. Generate the batch load program for each item type that objects will be loaded into. You can modify and execute the sample JCL jobs to generate a batch load program for any selected item type.

The ICMPBL02 batch load generation program does three things:

- a. It reads the item type and other options that you provided in the USERIN control file.
- b. It gets the definition of the item type from the Content Manager for z/OS system tables.
- c. It generates the source code of item type-specific subroutines for the batch load program. The generated source code is compiled and linked with other

existing Content Manager for z/OS library server modules to build a batch load program for the selected item type.

2. Prepare three input data files for the high-volume batch load program that you generated.

CTLDATA

Specifies the run control options and values to override system defaults, if needed.

OBJDATA

Contains the base part objects of the documents to be loaded.

IDXDATA

Specifies the size and metadata of the objects.

You can run the ICMMBLJ1 job to start the generated batch load utility after you complete these steps.

Important: The USERID of the ICMMBLJ1 job must be defined in IBM Content Manager with the **ClientImport** privilege or the **ItemSuperAccess** privilege. For each document to be loaded, the batch load program generates an ITEMID, assigns system values and user attribute values, then loads the values and the object into the Content Manager for z/OS database and OAM. The batch load program also performs auto-linking, event logging, and initiates an auto-start process for each document to be loaded if the item type is defined in Content Manager for z/OS with these features enabled. You can also choose to suppress these actions by using runtime parameters.

The high-volume batch load utility supports default system values based on IBM Content Manager and item type definitions. The batch load utility also supports a maximum object size up to the object size limitation of the Content Manager for z/OS resource manager. You can load objects into DB2 table partitions by generating ITEMID and COMPID based on the TIMESTAMP and CENTURY parameters. You can process up to 100 jobs by using parallel processing.

The Content Manager for z/OS high-volume batch load utility provides batch load capability for any item type. This function also supports many item type features, including:

- Auto-linking, auto start processing, and event logging
- Item types with or without child components
- Documents with multiple parts

This function supports many runtime options, including:

- Suppressing the item type features, or overriding default system control values
- Suppressing the storing of the object data, so only metadata is loaded
- Overriding system attribute values for individual items
- Linking an item to its folder by providing the folder ITEMID or by providing a linking rule
- Validating object data
- Converting input text object data from EBCDIC encoding to ASCII encoding, or loading EBCDIC or UNICODE text data
- Limiting the maximum length of VARCHAR and LOB column input
- Separating objects stored in OAM by using the options for OAM collection, management class, and storage class

- Using options for commit frequency, skip count, stop count, error handling, and trace functionality

Recommendation: Before you enable the high-volume batch load in a production environment, set TRACE=YES in the CTLDATA file and run the ICMMLJ1 job in your test environment to test the generated batch load program with the input data you prepared.

You must regenerate the batch load program for a given item type when any of the following conditions occur:

- The item type or its folder item type is updated with one or more additional attributes
- The default value of the item type is changed
- The folder definition that the load job links to is changed, for example, when the item type attribution or link attribution changes
- The auto-linking rule of the item type is changed
- A PTF contains Content Manager for z/OS high-volume batch load maintenance, and directs users to regenerate the load program

Related tasks

Installing the IBM Content Manager for z/OS high-volume batch load utility

Configuring the IBM Content Manager for z/OS high-volume batch load utility

Related reference

Limitations of the IBM Content Manager for z/OS high-volume batch load utility

Related information

"Troubleshooting batch load utility problems for Content Manager for z/OS" on page 623

Using the Content Manager for z/OS high-volume batch update utility

You must customize the sample high-volume batch update, delete, move, or link jobs, and you must generate the programs again when specific conditions occur. It is important to understand the supported functions of the high-volume batch update utility for the Content Manager for z/OS before you customize the sample jobs.

You can use the high-volume batch update utility to efficiently update, delete, move, or link large quantities of data in the Content Manager for z/OS library server and in the z/OS resource manager.

Tip: You can use the Content Manager for z/OS Job Configuration tool to configure jobs for the high-volume batch utility.

You do not need to prepare ITEMID or detailed attribute values for individual items to be updated, deleted, moved, or linked. Moving an object performs a reindexing operation.

You must complete two stages of configuration before running the batch update, delete, move, and link functions of the batch update utility:

1. Generate the ICMPBL04 batch update, delete, move, or link function that identifies all affected user tables and items. You can modify and run the sample ICMMLSU JCL jobs to generate an update, delete, move, or link function for any specified user table or item.

The ICMPBL04 batch update program generates the source code for the batch program that you specified in the CTLDATA file. The generated source code is compiled and linked with other existing Content Manager for z/OS library server modules to build a batch program for the selected user tables and items.

2. Prepare the input data files for the high-volume batch update program that you generated.

CTLDATA

Specifies the update, delete, move, or link function to perform on identified user tables or items. This file is required.

TBLDATA

Processes the SQL statement that you provided in the optional TBLDATA file, which refines the selected user tables list. This file is optional.

LOGDATA

Specifies an SQL statement that inserts user-specified data into a non-Content Manager user table. This file is optional.

OPTDATA

Specifies the optional processing parameter values, including whether to preview the affected user tables by using the Preparation mode, or update, delete, move, or link affected items by using the Execution mode. This file is optional.

You can run the ICMPBL02 job to start the generated batch utility functions after you complete these steps.

Important: The USERID of the ICMMBLJ2 sample job must be defined in Content Manager EE with the **AllPrivs** privilege.

Recommendation: Before you enable the high-volume batch update utility in a production environment, set RUNMODE=P in the OPTDATA file and run the ICMMBLJ2 job in your test environment to test the generated batch program with the input data, parameters, and options that you prepared.

You must customize the batch update, delete, move, or link functions that are generated before you use them. You also must be prepared to resolve any of the following situations:

- Include additional functions that are specific to your installation
- Specify an input format that is different from the default specification

You must regenerate the batch update, delete, move, or link programs when the following condition occurs:

- A PTF contains Content Manager for z/OS high-volume batch update maintenance, and directs users to regenerate the batch programs.

Deferring DDL execution

The purpose of this DDL (Data Definition Language) feature is to provide flexibility to a database administrator (DBA) or IBM Content Manager administrator. The administrator can defer the execution of data modeling modifications made in the IBM Content Manager library server. These modifications include:

- Creating, altering, or deleting an item type or component type.

- Defining, updating, or dropping indexes and text search indexes, foreign keys, and views.

Actions that merely change table data do not cause DDL entries, and cannot be deferred. These actions include adding a row (such as adding an item) or changing a row value (such as changing an attribute definition).

By enabling this feature, the IBM Content Manager administrator will be able to tailor DBA aspects of data modeling operations. For example, the administrator can define the tablespace in which user component tables, indexes, or views should be created.

When the IBM Content Manager administrator chooses to save the DDL entries for later execution, the IBM Content Manager data modeling operation behaves as follows:

1. The IBM Content Manager administrator creates an item type or component type using the system administration client or the Java API.
2. The definition, or metadata, of the item type and component type is stored in IBM Content Manager system tables.
3. IBM Content Manager generates three scripts that contain all database operations for that item type or component type. The scripts are named the same as the item type.
 - *ItemType* script: This is the main script that connects to the database. It invokes two other scripts, one with SQL DDL commands, another with DB2 Text Information Extender or DB2 Net Search Extender commands. This main script has a .bat extension on Windows and a .sh extension on UNIX.
 - *ItemType.DDL*: This script contains DDL statements to create the user component tables, corresponding indexes, and views in the database.
 - *ItemType_TIE* script: This script contains DB2 Text Information Extender and DB2 Net Search Extender drop indexes commands. This script has a .bat extension on Windows and a .sh extension on UNIX.

ItemType.log: This file is created after the scripts are executed. It contains the output of the database operations.
4. After executing the scripts, the item type or component type is ready for create, retrieve, update, and delete (CRUD) operations. This feature applies to the IBM Content Manager library server with DB2 UDB on the workstation.

Enabling the deferred DDL execution feature

The script is located in the *IBMCMROOT/config* directory and enables or disables the deferred DDL execution feature. By default, this feature is disabled.

AIX and Solaris

```
GenerateDDL.sh dbname userid password schema [1 | 0]
```

Windows

```
GenerateDDL.bat dbname userid password schema [1 | 0]
```

dbname

IBM Content Manager library server database name

userid User ID with DB2 administrator authority for this database

password

Password for the user ID

schema

IBM Content Manager library server database schema

1 or 0 1 enables and 0 disables the feature

Example: `GenerateDDL.bat icmnlbdb icmadmin password icmadmin 1.`

This feature can be enabled and disabled at any time. That is, after the feature is enabled, all data modeling operations for new and existing item types are saved in scripts. When the feature is disabled, data modeling operations for new and existing item types are applied immediately.

Scripts to create an item type

An IBM Content Manager administrator executes an IBM Content Manager data modeling operation, such as creating an item type `MyBook`, either using the system administration client or calling API. When the deferred DDL feature is enabled, the following scripts are created as a result of a data modeling operation:

MyBook.bat

This script executes the following operations:

1. Connect to the database.
2. Invoke the DB2 Text Information Extender or DB2 Net Search Extender script to drop the DB2 Text Information Extender or DB2 Net Search Extender indexes.
3. Invoke the DDL script.
4. Rename the DDL script to `ItemType.DDL.SAVE` and delete the DDL script.
5. Call `RebuildCompTypeForDDL` for each component that was modified or created.
6. Invoke DB2 Text Search commands to add/alter text search indexes.

Attention: On AIX or Solaris, the script has a `.sh` extension.

MyBook.DDL

Contains the DDL commands. It is invoked by the `MyBook.bat` or `MyBook.sh` script.

MyBook_TIE.bat

Contains the text search drop index command. It is invoked by `MyBook.bat`.

Attention: On AIX or Solaris, the script has a `.sh` extension.

RebuildCompTypeForDDL.class

This class file is deployed in the `IBMCROOT/config` directory and is called by the item type main script to generate the access modules. The input parameters are passed by the calling script.

Script Directory Location

All scripts created as a result of the DDL deferred execution feature are placed in the following location:

On AIX and Solaris `$IBMCADM_HOME/cmgmt/1s/DBName/UserDDL`

On Windows \$IBMCROOT/cmgmt/1s/DBName/UserDDL

where

dbname is the IBM Content Manager library server database name.

UserDDL is the directory created by IBM Content Manager when the deferred DDL execution feature is enabled.

Executing the scripts

The following script example uses a sample item type named MyBook.

Important: Ensure that the path for `IBMCROOT\lib\db2jcc.jar` is in your CLASSPATH.

1. The script created is:

- MyBook.bat (on Windows)
- MyBook.sh (on UNIX)

Usage is: `MyBook.bat dbhost dbport dbname userid password schema`

where:

dbhost IBM Content Manager library server database host name.

dbport IBM Content Manager library server database port number.

dbname

IBM Content Manager library server database name.

schema IBM Content Manager library server database schema.

2. The script can be executed after each data modeling operation. For example:
 - a. Define an item type.
 - b. Run the script for this item type.
 - c. The component is now ready for CRUD operations.
3. Optionally, the IBM Content Manager administrator can execute an *n* number of data modeling operations. Each data modeling operation is appended to the script and DDL file and all the operations are applied to the database when the script is run. For example:
 - a. Define an item type.
 - b. Modify the component by adding a new attribute.
 - c. Modify the component by setting it to be text searchable.
 - d. Add a new index to the component.
 - e. Create a new view on the component.
 - f. Run the script.
 - g. The item type is ready for CRUD (create, retrieve, update, and delete) operations.
4. After the script is executed, the DDL file is automatically deleted (a copy is saved as `script.DDL.SAVE`).
5. When a new data modeling operation is applied on that item type, a new set of script files is created.

Recommendation: After running a script, delete the *ItemType* and *ItemType_TIE* scripts.

Examining the logs

After executing the script, a log file is created with the output of the DDL and text search commands. Some SQL DDL drop statements are expected to show errors. For example, the drop command of a VIEW that precedes the CREATE statement of the same VIEW can show an error.

Re-running the script

If you must re-run the script, you must first rename the saved copy of the DDL to its original name. For example, rename *ItemType.DDL.SAVE* to *ItemType.DDL*.

Changing library server configurations when DDL deferred execution feature is enabled

Updating the following library server configuration parameters causes IBM Content Manager to drop and re-create the views. An update also causes IBM Content Manager to regenerate the access modules for all component types defined in IBM Content Manager, including the system-defined components such as document parts.

- Public Access Enabled
- ACL binding level
- Library ACL name

When changing any of these settings with the DDL deferred execution feature enabled, IBM Content Manager generates a script for each item type that is currently defined in the IBM Content Manager database. Scripts are generated for both user-defined and system-defined item types.

Make sure that you execute all the scripts that were generated as a result of changing the library server settings, or CRUD operations will fail. The execution of the scripts does not need to follow any particular order.

Allowing IBM Content Manager administrators without DB2 dbadm privilege to create the definition of data model objects

The deferred DDL execution feature enables IBM Content Manager users without the DB2 dbadm privilege to create the definition of data modeling objects. This action is possible because you first define the data modeling objects and save these definitions into a file. The actual execution of the scripts requires a user ID with the DB2 dbadm privilege. Follow these steps:

1. On the server where the library server is installed, go to the *IBMCMROOT\bind* directory.
2. Connect to the library server database as a DB2 administrator.
3. Open a DB2 command prompt.
4. At the DB2 command prompt, run the following commands, replacing *ICMCRLSDBSCHEMA* with the library server schema name:

```
bind icmplscp.bnd QUALIFIER ICMCRLSDBSCHEMA DYNAMICRULES  
BIND DATETIME ISO BLOCKING ALL  
bind icmplsti.bnd QUALIFIER ICMCRLSDBSCHEMA DYNAMICRULES  
BIND DATETIME ISO BLOCKING ALL  
bind icmplsiv.bnd QUALIFIER ICMCRLSDBSCHEMA DYNAMICRULES  
BIND DATETIME ISO BLOCKING ALL
```

```
bind icmplscv.bnd QUALIFIER ICMCRLSDBSCHEMA DYNAMICRULES
BIND DATETIME ISO BLOCKING ALL
bind icmplssc.bnd QUALIFIER ICMCRLSDBSCHEMA DYNAMICRULES
BIND DATETIME ISO BLOCKING ALL
```

5. Ensure that the IBM Content Manager user executing a data modeling operation using the system administration client is a system user.

The user executing the DDL script must have dbadm privilege. This scenario only works when the deferred DDL execution feature is enabled.

When disabling the deferred DDL execution feature, the following sequence of commands must be executed:

1. On the server where the library server is installed, go to the *IBMCMROOT\bind* directory.
2. Connect to the library server database as a DB2 administrator.
3. Open a DB2 command prompt.
4. At the DB2 command prompt, run the following commands, replacing *ICMCRLSDBSCHEMA* with the library server schema name:

```
bind icmplscp.bnd QUALIFIER ICMCRLSDBSCHEMA DATETIME ISO
BLOCKING ALL
bind icmplsti.bnd QUALIFIER ICMCRLSDBSCHEMA DATETIME ISO
BLOCKING AL
bind icmplsiv.bnd QUALIFIER ICMCRLSDBSCHEMA DATETIME ISO
BLOCKING ALL
bind icmplscv.bnd QUALIFIER ICMCRLSDBSCHEMA DATETIME ISO
BLOCKING ALL
bind icmplssc.bnd QUALIFIER ICMCRLSDBSCHEMA DATETIME ISO
BLOCKING ALL
```

Enabling the deferred DDL execution feature for Oracle

The deferred DDL (Data Definition Language) feature gives the database administrator (DBA) or IBM Content Manager administrator the option to defer the execution of data modeling modifications made in the IBM Content Manager library server.

The script to enable the deferred DDL execution feature, *@GenerateOraDDL.sql*, is located in the *IBMCMROOT/config* directory.

By default, the deferred DDL execution feature is disabled. To enable it, enter the following SQL command.

```
sqlplus SQLPlusConnectionString @GenerateOraDDL.sql 1
```

When the feature is enabled, IBM Content Manager creates the *itemtype.sql* script in the *IBMCMROOT/cmgmt/1s/dbname/UserDDL* directory. Additionally, IBM Content Manager saves all data modeling operations for new and existing item types in scripts.

To run the scripts, enter the following SQL command:

```
sqlplus SQLPlusConnectionString @itemType.sql LSName LSAdminUser LSAdminPassword
```

where:

LSName

IBM Content Manager library server database host name. For example, *icmnlsdb*.

LSAdminUser

IBM Content Manager library server administration user. For example, icmadmin.

To disable the deferred DDL execution feature, enter the same command but with a 0 instead of a 1. When the feature is disabled, data modeling operations for new and existing item types are applied immediately.

Comparison of IBM Content Manager workflow solutions

IBM Content Manager document routing, IBM Information Integrator for Content advanced workflow, and FileNet Business Process Manager integrated with IBM Content Manager provide the ability to create and manage workflow, but there are functional differences.

The following table summarizes the differences of the workflow solutions available with IBM Content Manager.

Attention: IBM Information Integrator for Content advanced workflow has been deprecated, and support will be removed in a future release.

Table 53. Functional comparison of Content Manager EE workflow solutions

Function	Document routing	Advanced workflow	FileNet Business Process Manager integrated with IBM Content Manager
Install and run the following software:	IBM Content Manager	<ul style="list-style-type: none"> • IBM Content Manager • WebSphere MQ • WebSphere MQ Workflow 	<ul style="list-style-type: none"> • IBM Content Manager • WebSphere MQ • IBM FileNet P8 Business Process Monitor • IBM Tivoli Directory Server
Authenticate users using:	<ul style="list-style-type: none"> • IBM Content Manager managed user ID and password • LDAP 	<ul style="list-style-type: none"> • IBM Content Manager managed user ID and password • LDAP 	LDAP
Install and run LDAP (required)			Supported
Model workflow processes in a graphical builder from the following operating systems:	<ul style="list-style-type: none"> • AIX • Linux • Solaris • Windows 	Windows only	<ul style="list-style-type: none"> • AIX • Linux • Solaris • Windows
Users interact with workflow processes using the following clients:	<ul style="list-style-type: none"> • Client for Windows • eClient • IBM WEBi • custom client 	<ul style="list-style-type: none"> • eClient • custom client 	<p>custom client only</p> <p>P8 Workplace or Workplace XT web applications cannot be used with IBM Content Manager content.</p>

Table 53. Functional comparison of Content Manager EE workflow solutions (continued)

Function	Document routing	Advanced workflow	FileNet Business Process Manager integrated with IBM Content Manager
Run workflow processes on the following operating systems:	<ul style="list-style-type: none"> • AIX • Linux • Solaris • Windows • z/OS 	<ul style="list-style-type: none"> • AIX • Solaris • Windows 	<ul style="list-style-type: none"> • AIX • Solaris • Windows
Administer workflow processes from a library server or system administration database using these database systems:	<ul style="list-style-type: none"> • DB2 • Oracle 	DB2 only	<ul style="list-style-type: none"> • DB2 • Oracle
Manage access to workflow processes, objects and worklists	Same as IBM Content Manager	Synchronize with WebSphere MQ Workflow server, which manages workflow authorization	Same as FileNet Business Process Manager
Develop applications that use workflow functionality with:	<ul style="list-style-type: none"> • C++ APIs • Java APIs • JavaBeans (non-visual) • Web services 	<ul style="list-style-type: none"> • C++ APIs • Java APIs • JavaBeans (non-visual) 	<ul style="list-style-type: none"> • Java APIs • Web services
Create parallel routes	Supported	Supported	Supported
Incorporate user exit routines and integrate with business applications	Supported	Supported	<p>Web services</p> <p>To add user exit routines, you must use the custom Step Processor.</p>
Create conditional routes	Supported	Supported	Supported
Create collection points	Supported	Federated datastore only	Collection points can be implemented using the WaitForConditions system step.
Define actions for users to complete in the client	Supported	Supported	Supported
Suspend and resume process	Supported	Supported	<p>Predefined time delay. Ad hoc suspend is not available.</p> <p>WaitForCondition system function is also available.</p>
Incorporate existing workflow processes as subprocesses	Supported	Supported	Supported

Table 53. Functional comparison of Content Manager EE workflow solutions (continued)

Function	Document routing	Advanced workflow	FileNet Business Process Manager integrated with IBM Content Manager
Route content over multiple content servers		Supported	Supported
Resolve and assign staff			Supported
Tooling:			Supported
• Business activity monitor			
• Process tracker			
• Process analyzer			
• Process simulation			

Managing document routing with IBM Content Manager

Document routing is a work management tool that you use to direct documents and folders from one user to another during the life cycle of a document.

Based on their privileges, users inspect documents and update them to complete a work step. For example, XYZ Insurance uses document routing for their auto claim process. In the process, work is directed from an insurance clerk to an underwriter. An underwriter waits for the police report and the insurance adjuster's damage assessment and then directs the claim to an insurance accountant or an underwriter assistant, depending on whether the underwriter approves or rejects the claim. Document routing allows XYZ Insurance to approve a claim without using paper or manually carrying a claimant's folder from one person to another.

End to end, deploying document routing consists of three high-level groups of tasks:

1. Plan a document routing process
2. Create a document routing process
3. Route documents (client users)

These three high-level groups contain the following specific tasks:

Plan a document routing process

The following illustration shows the overall task flow for document routing, with the planning tasks expanded.

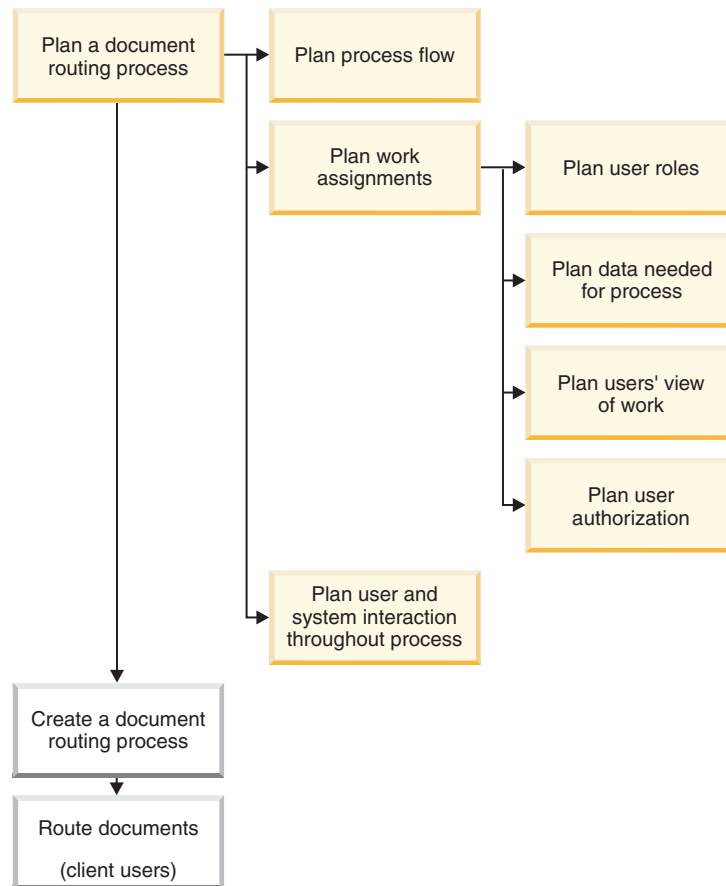


Figure 20. Common tasks for planning a document routing process

Create a document routing process

The following illustration shows the overall task flow for document routing, with the creation tasks expanded.

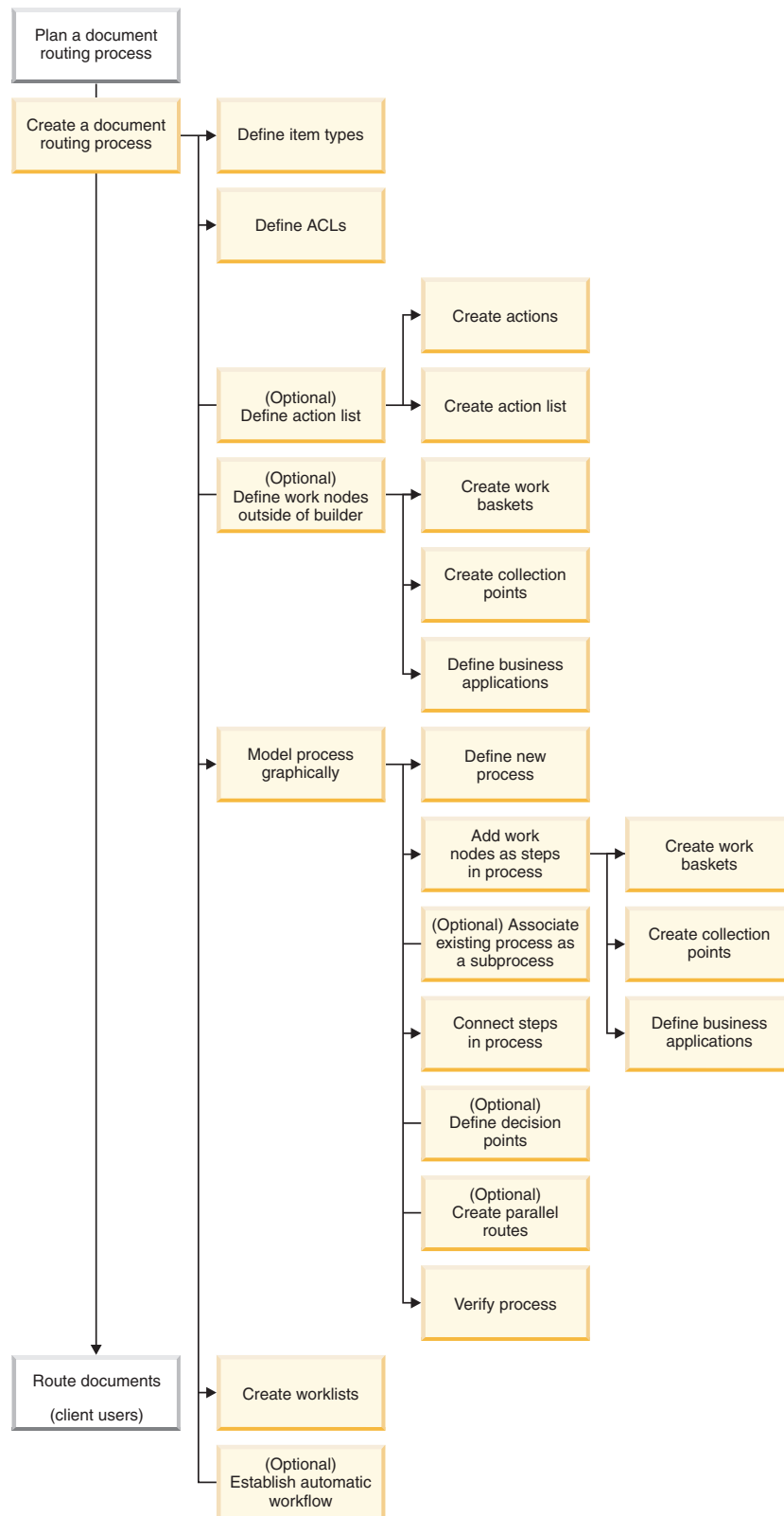


Figure 21. Common tasks for creating a document routing process

Route documents (client users)

These tasks are described in the Client for Windows and eClient help.

You can also use IBM WebSphere Application Server (or IBM WebSphere Business Integration Server Foundation) Process Choreographer to store document routing objects. See *Planning and Installing Your Content Management System* for more information.

Attention: The document routing function is an IBM Content Manager application that uses items to store document routing objects. The document routing objects are stored in IBM Content Manager as items and are managed using the standard CRUD (create, retrieve, update, and delete) APIs. The event logging for the item types is like any other item event. It includes the document routing items because they are just additional items.

“Planning a document routing process”

“Creating a document routing process” on page 265

Planning a document routing process

You can plan for document routing by completing the following tasks. The tasks are described in terms of an insurance scenario.

1. “Planning process flow”
2. “Planning work assignments” on page 258
3. “Planning user and system interaction throughout process” on page 264

Planning process flow

Create a flow diagram of the business process by understanding the goal of the business process and the required steps to reach the goal.

Before you begin to define a document routing process, you must analyze the work that your business performs, where and how it is performed, and by whom. An administrator or business analyst does this planning step.

Begin planning your document routing process by creating a paper flow diagram of the business process that you want to automate. You can begin with an abstract view of the process and then provide more detail as you interview the people who are involved in various steps of the process.

Consider how you want information and activities to flow. Where does the input originate? What is the final product? The final product might be the result of all the work accomplished by your business, by one department in your business, or by certain employees from different departments.

From your process flow diagram, you can also begin to identify the work nodes (work baskets, collection points, and business applications), any decision points, and any subprocesses required for your process. You can also identify points in your process where the process splits into parallel routes and then where it joins back into a single route. You define these document routing elements when you build your process, but you need to know what they are now so that you can plan the correct authorization for those elements.

Scenario: The XYZ Insurance Company has an automobile claim process for paperless claim processing. They have a well-defined, multiple step claims submission, review, and approval process that results in the claims being approved or rejected. The process involves agents, adjusters, underwriters, accountants, and assistants. The final product of the claims process is a check or rejection letter that is sent to the policy holder.

Figure 22 shows the claims process at a high level.

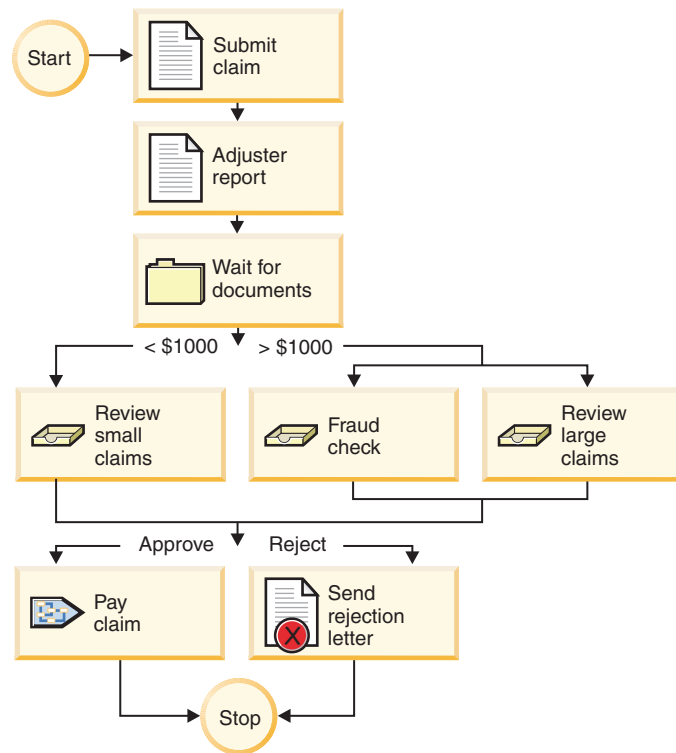


Figure 22. Flow diagram of the XYZ Insurance Company's claims process

The XYZ Insurance Company's claims process includes the seven steps described in Table 54.

Table 54. Steps in the XYZ Insurance Company's claims process

Step	Description	Corresponding flow diagram element	Necessary document routing elements
1	The process starts when an auto claim form is submitted, scanned and assigned by the system to a claim application folder based on the claim number and started on the auto claims process.	Start node	Start
2	The claim form inside the claim application folder is received by an insurance agent, who verifies the claim applicant's information and enters a claim amount value in the system.	Submit claim box	Work basket
3	The claim application folder is received and reviewed by the claims adjuster. The adjuster assesses the damage to the automobile, and submits a adjuster report with any pertinent photographs.	Adjuster report box	Work basket
4	The process waits for all claim application documents (including claim forms, adjuster reports, police reports, and automobile photos) to be added to the claim application folder before continuing.	Wait for documents box	Collection point

Table 54. Steps in the XYZ Insurance Company's claims process (continued)

Step	Description	Corresponding flow diagram element	Necessary document routing elements
5	<p>XYZ Insurance has two review processes for auto claims depending on the amount of the claim:</p> <p>Less than \$1000 If the claim is for less than \$1000, the claim undergoes a short review process. This alternative corresponds to the Review small claims box in the flowchart.</p> <p>More than \$1000 If the claim exceeds \$1000, then the claim undergoes a complete review. For a complete review, two routes occur simultaneously:</p> <ul style="list-style-type: none"> • The insurance claimant's background is checked for possible insurance fraud. The result of this search is stored in the system. • The second route is a full review by the underwriter, who reviews the claim application (including supporting documents) and approves or rejects the claim. 	Review small claims box or Fraud check and Review large claims boxes	<ul style="list-style-type: none"> • Decision point (claim amount) • Split large claim review • Business application (fraud check) • Work basket (underwriter review) • Join large claim review • Work basket (small claim review)
6	<p>The process branches depending on whether the claim was approved or rejected:</p> <p>Approval If the underwriter approved the claim application, the claim application folder proceeds to the accountant, who processes a check to pay for the claim submitted.</p> <p>Rejection If the underwriter rejected the claim application, the claim application folder proceeds to the assistant, who sends a rejection letter.</p>	Pay claim box or Send rejection letter box	Decision point, subprocess, work basket
7	The claim application folder proceeds to the end of the process.	Stop node	Stop

Planning work assignments

To plan work assignments, you complete four subtasks to identify the users of the process, what data they must manipulate during the process, how they interact with the process, and the authorization that they require.

1. "Planning user roles"
2. "Planning data needed for the process" on page 259
3. "Planning users' view of the work" on page 260
4. "Planning user authorization" on page 262

Planning user roles

Identify the types of users for the process.

From your process flow diagram, you can identify a list of the various user types that are required by the process. You can identify these user types by the role that they play in the process or by their job title. (The term *roles* is used here in a

generic sense rather than in the narrow sense of security terminology.) In some cases, these users interact with the process at a single step, in other cases, they interact with the process repeatedly.

Scenario: The XYZ Insurance Company's claim process involves the following five user types who each interact with the process at a single step:

Agents

Receive completed claim form from policy holder and enter pertinent information, such as claim amount, into the system.

Adjusters

Assess the damage to the automobile and submit an adjuster report with any pertinent photographs.

Underwriters

Review claims for amounts greater than \$1000 and approve or reject the claim.

Accountants

Generate a check request for approved claims.

Assistants

Notify policy holders of rejected claims.

Planning data needed for the process

Plan the item types required for the process and the necessary privileges to work with them.

From your process flow diagram, you can identify the data that flows through your process, such as documents and folders. You must identify the necessary item types for that data.

If you are modeling a business process that includes some data that is online (for example, scanned documents), you might be able to use some existing item types. Alternatively, you might decide to create all new item types for use in the process to separate it from your other data. Creating new item types might make it easier for you to control authorization for the process.

If your process includes a collection point (a place where the process waits for documents or information to arrive), your users must define a folder. The folder ultimately contains the various documents that are awaited at the collection point and then travels with them as the process continues. Your users must link an item in a folder (containment) relationship with one or more items to include within it.

You might also consider using auto-linking. When you establish auto-linking between item types and an item is created of one item type, an item of the auto-linked item type is automatically created and linked. For example, using the item types described below, you might auto-link the ClaimForm item type in a containment relationship with the ClaimFolder item type. When a user creates an item of the ClaimForm type, an item of the ClaimFolder type is created automatically and linked as a container of the ClaimForm item.

Recommendation: Keep a list of the item types and work node variables that you use in your process, particularly those that you use in a decision point or a collection point. The library server does not restrict you from deleting item types or work node variables that are used in decision points or collection points.

Scenario: The XYZ Insurance Company's claim process involves the following five item types:

ClaimForm

Claim request, which is completed by the policy holder, accepted by the agent, and reviewed by the adjuster. Depending on the amount of the claim, this form might be reviewed and approved or rejected by the underwriter. The claim form is viewed by either the accountant or the assistant.

ClaimFolder

Folder that initially contains only the claim form. Throughout the process, the other documents are added: the adjuster's report, the police report, and photos.

This item type is required for the collection point in the process. Users must instantiate items of ClaimFolder type as folders, not as documents, to be usable at the collection point. Users instantiate items of the other item types (ClaimForm, AdjusterRpt, PoliceRpt, and AutoPhoto) as documents that are contained within the ClaimFolder item.

AdjusterRpt

Report of the assessment of the damage by the adjuster; it is added to the claim folder when available.

PoliceRpt

Official report of the accident, which might not be available for all claims; it is added to the claim folder when available.

AutoPhoto

Photos of the damage by the adjuster; they are added to the claim folder when available.

"Sample: Privileges for item types" on page 267 provides a matrix of the users of the XYZ Insurance Company's claim process and the item types that flow through the process. As you can see from the table, for the item types, the agent and adjuster must have the privileges included in the ClientTaskAll system-defined privilege group.

The underwriter, accountant, and assistant must each have the privileges in the following two system-defined privilege groups: ClientTaskView and ClientTaskUpdate.

Related concepts

"Auto-linking" on page 188

Planning users' view of the work

Plan the worklists, which users view to work with one or more processes, and plan the necessary privileges.

From the eClient, Client for Windows, or a custom client, your users interact with the process from their worklist, which is a filter of the work that is associated with one or more work nodes in a single process, or multiple processes.

To adequately plan your worklist, you must understand the intricacies of access control lists (ACL). The worklist has an associated access control list (ACL), as do work nodes and the documents or folders being routed in the work packages. Table 55 on page 261 describes where you code ACLs to control access to elements in a document routing process.

Table 55. ACLs that control document routing elements

The ACL for the:	Controls:
Worklist	Who can use this worklist to filter work packages that originated from the work nodes specified for this worklist.
Document or folder being routed in the work package	Who can retrieve that work package
Work node	Who can update work package properties (including suspending or resuming it) at that work node

The intersection of a user's privilege set and the worklist ACL controls who can view and work with that worklist. Additionally, if you want users to retrieve and work with work packages, you must also ensure that the users have read or update access to the data in that work package. If users do not have access to a routed document, they cannot see the work package that carries it.

Table 56 describes the privileges you must grant for common activities during document routing processes.

Table 56. Required privileges for document routing activities

If you want users to be able to:	Grant these privileges:	For these entities:
View work packages	Read	Document to view, work node where they should view it, worklist
Update work packages	Update	Work node where user should be able to update the work package
	Read	Document and worklist
Update documents	Update	Document to update
	Read	Work node and worklist

If you create a worklist that combines multiple work nodes in a single process, or if you include work nodes from other processes, your authorization decisions become more complicated. To simplify authorization, you might decide to create a worklist for each individual work node, or to create a worklist that applies to all work nodes in a process that include work that is assigned to a specific user role. Know also that if you use a single worklist to combine the work at multiple work nodes, you might confuse your user, who might not have as clear a sense of where they are in the process as they work down their worklist.

Whether you include single or multiple work nodes in the worklist, you can prioritize the work that displays in that worklist according to priority or date. You can also filter the work. For example, you might create a worklist that filters all work that has a notification flag set (work that has waited too long at a single work node or spent too much time in the process as a whole), so that a certain user type can review and act on work that is overdue.

Plan how you want your users to interact with the process. Determine whether you want them to review the work assigned to them at each work node, or multiple work nodes. Determine whether you need additional worklists for monitoring the process (for overdue or suspended work).

Scenario: In the XYZ Insurance Company's claim process, the user types interact with the process at single work nodes. In this case, creating a worklist by user type automatically means that each worklist includes a single work node. XYZ Insurance decides on the following five worklists:

- AgentWL
- AdjusterWL
- UnderwriterWL
- AccountantWL
- AssistantWL

“Sample: Privileges for worklists” on page 268 provides a matrix of the users of the XYZ Insurance Company's claim process and their associated worklists. As you can see from the table, each of the five user types must have the privileges in the ClientTaskUpdate, ClientTaskView, and ClientTaskDocRouting privilege groups.

Planning user authorization

Use the work of previous planning tasks to build matrices that you can use to plan privileges for all aspects of the process.

After you have a list of all of the users of your process, and all of the elements of your process, you must determine the privileges that your users need to work with the process. You must be able to authorize your users to work with:

The process

Specifically, to start, end, suspend, or resume the process.

The steps of the process

Specifically, to route the work from one work node to another.

The data that flows through the process

Specifically, to get and update work packages and to work with the worklist. Because the work packages contain items (documents or folders), you must also ensure that your users have the necessary privileges to work with those items.

IBM Content Manager provides the document routing privileges and their associated privilege sets and privilege groups that are summarized in Table 57.

Table 57. System-defined privileges that are specifically related to document routing

These system-defined privileges:	Provide the ability to:	Are included in these system-defined privilege sets for client users:	And these system-defined privilege groups for client users:
ItemGetWork	Retrieve work packages	<ul style="list-style-type: none"> • ClientUserEdit • ClientUserReadOnly • ClientUserAllPrivs 	<ul style="list-style-type: none"> • ClientTaskDocRouting • ClientTaskAll
ItemGetWorkList	Retrieve worklists	<ul style="list-style-type: none"> • ClientUserEdit • ClientUserReadOnly • ClientUserAllPrivs 	<ul style="list-style-type: none"> • ClientTaskDocRouting • ClientTaskAll
ItemRoute	Route a work package from one work node to another	<ul style="list-style-type: none"> • ClientUserEdit • ClientUserAllPrivs 	<ul style="list-style-type: none"> • ClientTaskDocRouting • ClientTaskAll

Table 57. System-defined privileges that are specifically related to document routing (continued)

These system-defined privileges:	Provide the ability to:	Are included in these system-defined privilege sets for client users:	And these system-defined privilege groups for client users:
ItemRouteStart	Start a document routing process	<ul style="list-style-type: none"> ClientUserEdit ClientUserCreateAndDelete ClientUserAllPrivs 	<ul style="list-style-type: none"> ClientTaskDocRouting ClientTaskAll
ItemRouteEnd	End a document routing process at any point in the process	<ul style="list-style-type: none"> ClientUserEdit ClientUserAllPrivs 	<ul style="list-style-type: none"> ClientTaskDocRouting ClientTaskAll
ItemUpdateWork	Suspend or resume a work package at a work node or change the priority of a work package	<ul style="list-style-type: none"> ClientUserEdit ClientUserAllPrivs 	<ul style="list-style-type: none"> ClientTaskDocRouting ClientTaskAll
ItemGetAssignedWork	Retrieve work packages assigned to another user	<ul style="list-style-type: none"> ClientUserAllPrivs 	<ul style="list-style-type: none"> ClientTaskAll

The easiest way to determine the required privileges is to create matrices of users and the various elements so that you can identify the necessary privileges at the intersection of each user with each element.

In addition to the privilege sets that you assign your users, you must also assign access control lists (ACLs) to most elements of the document routing process (the process, the work nodes, the associated worklists, and the actual data that is inside of the work packages that flow through the process). The intersection of a user's assigned privilege set and the access control list for a document routing element is what determines what that user can do. Table 58 identifies the ACLs and privileges that the library server checks for each document routing activity.

Table 58. Document routing authorization checking

Document routing activity	For authorization, library server checks ACL of:	And the user's privilege set for this privilege ¹ :
Start a process	Process	ItemRouteStart
Retrieve a work package from a work node	Item type of the item that is in the work package ²	ItemGetWork
Suspend or resume a process	Work node at which the suspension or resumption is to occur	ItemUpdateWork
Route work package from one work node to another	Work node from which work is routed (starting work node)	ItemRoute
End a process prematurely	Work node in which the item resides	ItemRouteEnd
Retrieve worklist	Worklist	ItemGetWorkList

Notes:

1. This column uses the system-defined privileges, but you can create your own.
2. Assuming that you accepted the default ACL checking at the item type level when you created the item type.

Table 59 provides examples based on the intersecting privileges summarized in Table 58 on page 263. Each row of the table is a separate example.

Table 59. Privilege and access control examples

User wants to:	Library server checks ACL on:	Required privilege:	User's privilege set includes privilege?	User can complete the task, if these ACL conditions are true:
Start an item on Process1	Process1	ItemRouteStart	Yes	ACL includes the user (or a group that includes the user) associated with a privilege set that includes the ItemRouteStart privilege.
Retrieve work package WP1 from work node WN1	Item type in WP1	ItemGetWork	Yes	ACL includes the user (or a group that includes the user) associated with a privilege set that includes the ItemGetWork privilege.
Suspend work package WP1 at work node WN2	WN2	ItemUpdateWork	Yes	ACL includes the user (or a group that includes the user) associated with a privilege set that includes the ItemUpdateWork privilege.
Route work package WP1 from work node WN1 to work node WN2	WN1	ItemRoute	Yes	ACL includes the user (or a group that includes the user) associated with a privilege set that includes the ItemRoute privilege.
Route work package WP1 from work node WN1 to work node WN2	WN1	ItemRoute	No	ACL contents are moot, because the user's privilege set does not include the necessary ItemRoute privilege

Scenario: “Sample: Privileges for work nodes” on page 268 shows the matrix for XYZ Insurance Company users and the work nodes in the claims process. You do not need to assign privileges for decisions points.

“Planning data needed for the process” on page 259 described the matrix for the XYZ Insurance Company users and item types. “Planning users' view of the work” on page 260 described the matrix for the XYZ Insurance Company users and their worklists.

Planning user and system interaction throughout process

Plan when and how the users are prompted for input during the process.

At work baskets and collection points during the process, you can prompt users to enter values or responses. During the process, you can test the values that users enter (work node variables), attribute values for the item or items being routed, or the properties of the work package. Based on the test results, you can alter the flow of work through the process accordingly.

Identify whether there are points in your process where you require input from the user. Are there values or information that cannot be known when the data is initially created and started on the process? Are there responses to questions that might change each time through the process that affect the flow of work? Do routes exist for escalated work or for controlled termination of invalid work?

For each time that you require user input, identify what type of value or response you are looking for. Is there a default value? Is user input required or not?

Scenario: In the XYZ Insurance Company's claim process, the agent must enter a value, ClaimAmount, when ensuring that all of the necessary paperwork is available and completed correctly. The ClaimAmount value is used later in the process to determine whether the claim follows a minimal review (less than \$1000) or a full review (more than \$1000). The agent must enter this value because the process cannot complete without it.

Creating a document routing process

To create a document routing process, you complete the following tasks. Most of the work to create the process is completed inside of the graphical process builder. However, as summarized in the task list, before you can begin creating a process in the builder, you must create the necessary item types and set up the necessary access control and privileges.

1. "Prerequisite tasks"
2. Optional: "Defining an action list" on page 269
3. Optional: "Defining work nodes outside of the graphical process builder" on page 275
4. "Modeling the process graphically" on page 294
5. "Creating a worklist" on page 312
6. Optional: "Establishing automatic workflow" on page 317

Prerequisite tasks

Before you can create a document routing process, you must complete these tasks: define necessary item types and define the required access control lists.

1. "Defining item types"
2. "Defining access control lists"

Defining item types

Define the item types for the items that you want to route through the process.

Before you can begin building your process, you must define the item types for the work that you will route through the process. If you completed the planning tasks, you already have a list of these item types.

Ultimately, you might decide to establish automatic workflow for some of these item types, which means that when new items are created of that item type, they are automatically started on your document routing process. However, you cannot establish automatic workflow until after you create the document routing process. At that time you can go back and modify the appropriate item types.

Related tasks

"Creating an item type" on page 153

Defining access control lists

Define the access control lists that you need for all elements of the process.

When you have a complete picture of the elements of your process, you can design the access control lists that you need. In a document routing process, you use access control lists (ACLs) to allow appropriate users to access the elements of the process at appropriate times. You can apply an ACL to any of the following document routing process elements: item types, work nodes, worklists, and the process itself.

The following steps provide one way to determine the ACLs that you need for your process.

1. Identify user groups who are involved with this process. For the XYZ Insurance Company's claims process, you need the following user groups:
 - Agent
 - Adjuster
 - Underwriter
 - Accountant
 - Assistant
2. Identify IBM Content Manager elements (item types, process, work nodes, worklists, and so forth) that the users must access during the process. If you completed the planning tasks, you should have this list available. "Sample: Required elements for the insurance scenario" on page 267 provides a list of the user groups and the elements required for the XYZ Insurance Company's claim process.
3. Create a matrix of the user groups and the elements.
4. In each cell of the matrix, identify the privileges that are required during the process execution, such as CRUD (create, retrieve, update, and delete) capabilities. "Sample: Privileges for item types" on page 267 provides the item type matrix for the insurance scenario. "Sample: Privileges for work nodes" on page 268 provides the work node matrix. "Sample: Privileges for worklists" on page 268 provides the worklist matrix.
5. Represent the required privileges as privilege groups, either privilege groups provided by the product, or those defined by you. The linked samples identify the system-defined privilege groups required for each permutation identified in the matrix.
6. Grant privileges for the process as a whole.
 - To be able to start the process, the appropriate users must have ItemRouteStart privilege.
 - All of the user groups need R (ClientTaskView) privileges for the process as a whole, which is called ClaimsProcess in the scenario.
 - Also in the scenario, the ClaimsProcess includes a PayClaim subprocess, for which the accountant requires R (ClientTaskView) privileges.
7. Define access control lists for each of the IBM Content Manager entities and for the process as a whole. You can choose to share access control lists for different entities. "Sample: Required ACLs" on page 268 maps the access requirements for each entity to an access control list.

Related concepts

“Access control lists” on page 472

“Privilege groups” on page 514

Related tasks

“Creating privileges” on page 477

“Creating privilege groups” on page 513

“Creating access control lists” on page 471

Related reference

“Predefined privileges” on page 477

“Privilege group members” on page 514

Related information

“Defining privileges, privilege groups, and privilege sets” on page 476

Sample: Required elements for the insurance scenario: Table 60 summarizes the users, item types, work nodes, worklists that are required for the XYZ Insurance Company's claims process.

Table 60. User groups and entities required for the insurance document routing process

User groups	Item types	Work nodes	Worklists	Processes
Agent	ClaimForm	SubmitClaim	AgentWL	ClaimsProcess
Adjuster	ClaimFolder	AdjusterReport	AdjusterWL	PayClaim
Underwriter	AdjusterRpt	WaitForDocuments	UnderwriterWL	
Accountant	PoliceRpt	ReviewSmallClaim	AccountantWL	
Assistant	AutoPhoto	ReviewLargeClaim	AssistantWL	
		FraudCheck		
		SendRejectionLetter		

Sample: Privileges for item types: Table 61 identifies the privileges that each user group needs for each of the item types that are used in the process. In the table, the letters CRUD represent create, retrieve, update, and delete privileges, respectively.

Table 61. User group privileges required for each item type

User group	ClaimForm	ClaimFolder	AdjusterRpt	PoliceRpt	AutoPhoto
Agent	CRUD	CRU	R	R	R
Adjuster	CRU	CRU	CRUD	R	R
Underwriter	R	RU	R	R	R
Accountant	R	RU	R	R	R
Assistant	R	RU	R	R	R

Corresponding system-defined privilege groups:

CRUD ClientTaskAll

CRU ClientTaskCreate, ClientTaskView, and ClientTaskUpdate

RU ClientTaskView and ClientTaskUpdate

R ClientTaskView

Sample: Privileges for work nodes: Table 62 identifies the privileges that each user group needs for each of the work nodes that is used in the process. In the table, the letter R represents read privileges and U represents update privileges.

Table 62. User group privileges required for each work node

Work node	Agent	Adjuster	Underwriter	Accountant	Assistant
SubmitClaim	RU				
AdjustReport		R			
WaitForDocuments	R	R			
ReviewSmallClaim			R		
ReviewLargeClaim			R		
FraudCheck			R		
SendRejectionLetter					R
Corresponding system-defined privilege groups:					
RU	ClientTaskUpdate, ClientTaskView, and ClientTaskDocRouting				
R	ClientTaskView and ClientTaskDocRouting				

Sample: Privileges for worklists: Table 63 identifies the privileges that each user group needs for each of the worklists that are used in the process. In the table, the letters RU represent read and update privileges respectively.

Table 63. User group privileges required for each worklist

User group	AgentWL	AdjusterWL	UnderwriterWL	AccountantWL	AssitantWL
Agent	RU				
Adjuster		RU			
Underwriter			RU		
Accountant				RU	
Assistant					RU
Corresponding system-defined privilege groups:					
RU	ClientTaskUpdate, ClientTaskView, and ClientTaskDocRouting				

Sample: Required ACLs: Based on the privileges required, you can decide on the access control for each of the item types, work nodes, worklists, and the processes required for your document routing process. In this scenario, each of the entities has its own ACL, as shown in Table 64.

Table 64. Access control lists required for each entity

Entity	User group	Access control list
ClaimFolder	All	ClaimFolderACL
ClaimForm	All	ClaimFormACL
AdjusterRpt	All	AdjusterRptACL
PoliceRpt	All	PoliceRptACL
AutoPhoto	All	AutoPhotoACL
SubmitClaim	Agent	AgentReadWBACL
AdjusterReport	Adjuster	AdjusterReadWBACL
WaitForDocuments	Agent, Adjuster	AgentAdjusterReadCPACL

Table 64. Access control lists required for each entity (continued)

Entity	User group	Access control list
ReviewSmallClaim	Underwriter	UnderwriterReadWBACL
ReviewLargeClaim	Underwriter	UnderwriterReadWBACL
SendRejectionLetter	Assistant	AssistantReadWBACL
AgentsWL	Agent	AgentWLACL
AdjusterWL	Adjuster	AdjusterWLACL
UnderwriterWL	Underwriter	UnderwriterWLACL
AccountantWL	Accountant	AccountantWLACL
AssistantWL	Assistant	AssistantWLACL
PayClaim	Accountant	PayClaimACL
ClaimsProcess	All	ClaimsProcessACL

Defining an action list

Optional: Define an action list if you want to identify specific actions for client users to perform during the steps in your process. You can select from a set of predefined actions and create your own actions. The actions that you create become menu choices that client users can select while working with your process. Although you are not required to define an action list, if you do not, your users see only menu choices related to the available routes for the work package; these route names might be cryptic.

1. Optional: "Creating an action"
2. Optional: "Creating an action list" on page 274

Creating an action

Create actions that users can perform during the steps in the process.

You can create an action by completing the following steps:

1. Click **Document Routing** from the tree view in the System Administration Client window.
2. Right-click **Actions** and then **New**. The New Action window opens.
3. Type a name for your action in the **Name** field. The name can be up to 32 alphanumeric characters. You cannot change the name after you create the action.
4. Optional: In the **Description** field, type a description (up to 254 characters) of the action. Descriptions are helpful when you create a specialized action, for example, an action that applies to a specific set of documents and work packages. You might also want to include a description for actions that you can use at any time. Descriptions help you to differentiate your purposes for creating one action one way over another way.
The description that you type here displays in the system administration client when you view details.
5. Optional: Type an alphanumeric name in the **Display name** field. This name displays to Client for Windows and eClient users as a menu choice, so you should make the name short and meaningful.
6. Optional: In the **Shortcut** field, type the keys that give users quick access to the action in a custom client. This shortcut also displays in the custom client menu.

Restriction: Shortcut settings in this field do not apply to the eClient or Client for Windows, only to custom clients.

7. Optional: Select an icon for your action in the **Icon** field. If you do not know where the graphic file is located or what it is called, click **Choose file**. Click **Preview** to see what the graphic looks like.

Restriction: You cannot select an icon if your library server database is on Oracle.

8. Specify the JavaServer Pages application, link library, or function for this action based on where it will run.
 - a. Select the client application types that you want to use this action.

Application type:	Select if your users use:
Web client	eClient or a custom Web-based client
Desktop client	Client for Windows or a custom desktop client
Both	Both types of application, whether IBM or custom

- b. Depending on the application type you selected, you might need to provide information in one, two, or three of the following fields.

Field:	Available when you select:	Value to enter:	Example:
Application name	Web client or Both	Full file name of the JavaServer Pages application that runs on the Web client application	ProcessClaims.jsp
Link library name	Desktop client or Both	Full file name of the DLL that runs on the desktop client application	ProcessClaims.dll
Function name	Desktop client or Both	File name of the function that runs on the desktop client application	ProcessClaims

9. Click **OK** to create your action and close the window. Click **Apply** to save the action and keep the window open to create another action.

Action:

An *action* specifies how a user can manipulate the work packages at a work node.

You can create your own actions, or use any of the following system-defined actions:

CMclient_Start on Process

Users select this action to start a work package on a document routing process.

CMclient_Remove from Process

Users select this action to remove a work package that is currently on a document routing process from that process.

CMclient_Change Process

Users select this action to remove a work package from one document routing process and start it on another process.

CMclientChange Priority

Users select this action to change the priority of the selected document routing process.

CMclient_View Process info

Users select this action to view information about a selected document routing process.

CMclient_View Process variables

Users select this action to view variable information about a selected document routing process.

CMclient_Change Owner

Users select this action to change the owner of the selected document routing process.

CMclient_Suspend

Users select this action to suspend a work package in the document routing process that it is currently on.

CMclient_Resume

Users select this action so that a suspended work package can resume moving through the document routing process that it is currently on.

After you create an action, you must include it in an action list to use it.

Viewing or modifying an action:**Restrictions:**

- You cannot change the name of the action.
- You can modify only the description and display name for a system-defined action.

To view or modify an action that you previously defined:

1. Click **Document Routing** from the tree view in the System Administration Client window.
2. Click **Actions** and then right-click a predefined action and click **Properties**. The Action Properties window opens.
3. Optional: In the **Description** field, type or edit the description (up to 254 characters) of the action. Descriptions are helpful when you create a specialized action, for example, an action that applies to a specific set of documents and work packages. You might also want to include a description for actions that you can use at any time. Descriptions help you to differentiate your purposes for creating one action one way over another way.
The description that you type here displays in the system administration client when you view details.
4. Optional: Type an alphanumeric name in the **Display name** field. This name displays to Client for Windows and eClient users as a menu choice, so you should make the name short and meaningful.
5. Optional: In the **Shortcut** field, type the keys that give users quick access to the action in a custom client. This shortcut also displays in the custom client menu.

Restriction: Shortcut settings in this field do not apply to the eClient or Client for Windows, only to custom clients.

6. Optional: Select an icon for your action in the **Icon** field. If you do not know where the graphic file is located or what it is called, click **Choose file**. Click **Preview** to see what the graphic looks like.

Restriction: You cannot select an icon if your library server database is on Oracle.

7. Specify the JavaServer Pages application, link library, or function for this action based on where it will run.
 - a. Select the client application types that you want to use this action.

Application type:	Select if your users use:
Web client	eClient or a custom Web-based client
Desktop client	Client for Windows or a custom desktop client
Both	Both types of application, whether IBM or custom

- b. Depending on the application type you selected, you might need to provide information in one, two, or three of the following fields.

Field:	Available when you select:	Value to enter:	Example:
Application name	Web client or Both	Full file name of the JavaServer Pages application that runs on the Web client application	ProcessClaims.jsp
Link library name	Desktop client or Both	Full file name of the DLL that runs on the desktop client application	ProcessClaims.dll
Function name	Desktop client or Both	File name of the function that runs on the desktop client application	ProcessClaims

8. Click **OK** to save the changes to the action. Click **Apply** to save the action and keep the window open to create, modify, or view another action.

Copying an action:

Restriction: You cannot copy a system-defined action.

To copy an action, complete the following steps:

1. Click **Document Routing** from the tree view in the System Administration Client window.
2. Click **Actions** and then right-click a predefined action and click **Copy**. The Copy Action window opens.
3. Enter a name for your action in the **Name** field. The name can be up to 32 alphanumeric characters. You cannot change the name after you create the action.

4. Optional: In the **Description** field, type a description (up to 254 characters) of the action. Descriptions are helpful when you create a specialized action, for example, an action that applies to a specific set of documents and work packages. You might also want to include a description for actions that you can use at any time. Descriptions help you to differentiate your purposes for creating one action one way over another way.

The description that you type here displays in the system administration client when you view details.

5. Optional: Type an alphanumeric name in the **Display name** field. This name displays to Client for Windows and eClient users as a menu choice, so you should make the name short and meaningful.
6. Optional: In the **Shortcut** field, type the keys that give users quick access to the action in a custom client. This shortcut also displays in the custom client menu.

Restriction: Shortcut settings in this field do not apply to the eClient or Client for Windows, only to custom clients.

7. Optional: Select an icon for your action in the **Icon** field. If you do not know where the graphic file is located or what it is called, click **Choose file**. Click **Preview** to see what the graphic looks like.

Restriction: You cannot select an icon if your library server database is on Oracle.

8. Specify the JavaServer Pages application, link library, or function for this action based on where it will run.
- a. Select the client application types that you want to use this action.

Application type:	Select if your users use:
Web client	eClient or a custom Web-based client
Desktop client	Client for Windows or a custom desktop client
Both	Both types of application, whether IBM or custom

- b. Depending on the application type you selected, you might need to provide information in one, two, or three of the following fields.

Field:	Available when you select:	Value to enter:	Example:
Application name	Web client or Both	Full file name of the JavaServer Pages application that runs on the Web client application	ProcessClaims.jsp
Link library name	Desktop client or Both	Full file name of the DLL that runs on the desktop client application	ProcessClaims.dll
Function name	Desktop client or Both	File name of the function that runs on the desktop client application	ProcessClaims

9. Click **OK** to create your action and close the window. Click **Apply** to save the action and keep the window open to create another action.

Creating an action list

Build an action list from system-defined actions and actions that you created. If you choose to create an action list, you apply it to one or more work nodes in your process. You can create multiple action lists.

To create an action list, complete the following steps:

1. Click **Document Routing** from the tree view in the System Administration Client window.
2. Right-click **Action lists** and then **New**. The New Action List window opens.
3. Enter a name for your action list in the **Name** field. The name can be up to 32 alphanumeric characters. You cannot change the name after you create the action list.
4. Optional: In the **Description** field, type a description (up to 254 characters) of the action list. The description that you type here displays in the system administration client when you view details.
5. Populate the list of actions on the right. You can select multiple actions by holding the Ctrl key and clicking each action.
 - Add a selected action from the left list to the right by clicking **Add**.
 - Remove an action from the right list to the left by clicking **Remove**.
 - Use the search fields to search for actions to add or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
6. Optional: You can create additional actions by clicking **Create New Action**.
7. When you finish defining the new action list, click **OK** or **Apply**.

Action list: An *action list* is a list of actions that a user can perform on work packages.

You can assign an action list to a work node (work basket, collection point, or business application) to specify the actions that the user can take at that step in the process. When a work package reaches a work node that has an assigned action list, a client application can retrieve the action list and show all of the actions that a user can select.

Consider what actions you want your users to take on the contents of a work package during the document routing process. For example, a claims adjuster can accept a claims form or reject it as incomplete.

If your company is using the Client for Windows or eClient, the actions that you specify display in the clients as pop-up menu choices. If you do not assign an action list to a work node, the menu choices are limited to the names of the paths that proceed from that work node in the process.

If you choose to apply an action list, it must be a comprehensive list of all actions performed on a work package or its contents.

Viewing or modifying an action list:

You need to ensure that your system has the most current actions available to your users. If policies change in your business, you need to update action lists that you created in the past. You might also need to check the current state of action lists to see what actions they include.

To view or modify a predefined action list:

1. Click **Document Routing** from the tree view in the System Administration Client window.
2. Click **Action lists** and then right-click a predefined action list and click **Properties**.
3. Optional: In the **Description** field, type a description (up to 254 characters) of the action list. The description that you type here displays in the system administration client when you view details.
4. Edit the list of actions on the right. You can select multiple actions by holding the Ctrl key and clicking each action.
 - Add a selected action from the left list to the right by clicking **Add**.
 - Remove an action from the right list to the left by clicking **Remove**.
 - Use the search fields to search for actions to add or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
5. Optional: You can create additional actions by clicking **Create New Action**.
6. When you finish viewing or modifying the action list, click **OK** or **Apply**.

Copying an action list:

Copy an action list when you want to create an action list that has similar actions, or, if you want to rename a current action list.

To copy an action list, complete the following steps:

1. Click **Document Routing** from the tree view in the System Administration Client window.
2. Click **Action lists** and then right-click a predefined action list and click **Copy**. The Copy Action List window opens.
3. Enter a name for your action list in the **Name** field. The name can be up to 32 alphanumeric characters. You cannot change the name after you create the action list.
4. Optional: In the **Description** field, type a description (up to 254 characters) of the action list. The description that you type here displays in the system administration client when you view details.
5. Edit the list of actions on the right. You can select multiple actions by holding the Ctrl key and clicking each action.
 - Add a selected action from the left list to the right by clicking **Add**.
 - Remove an action from the right list to the left by clicking **Remove**.
 - Use the search fields to search for actions to add or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
6. Optional: You can create additional actions by clicking **Create New Action**.
7. When you finish defining the new action list, click **OK** or **Apply**.

Defining work nodes outside of the graphical process builder

You can define work nodes before you begin to model your process in the graphical process builder or you can define them while you model your process.

You must define the necessary access control list or lists for this work node before you can create the work node.

To create a work node outside of the graphical process builder:

1. Expand **Document Routing** in the tree view.
2. Right-click the type of work node that you want to create (**Work Basket**, **Collection Point**, or **Business Application**) and click **New**. The New Work Basket, New Collection Point, or New Business Application window opens.
3. Complete the fields to create the work node.
 - “Creating a work basket”
 - “Creating a collection point” on page 283
 - “Defining a business application” on page 291

Because work nodes can exist in more than one process, you can copy, view, modify, or delete work nodes only outside of the graphical process builder. Right-click the work node and select the relevant menu item.

Work node

A *work node* is a step within a document routing process at which items wait for actions to be completed by end users or applications, or through which items move automatically. Work node is the generic term for one of the following three types of work nodes:

- Work basket
- Collection point
- Business application

You must give each work node that you create a name and an access control list. After you decide the name and access control list, you can optionally determine what user exit function the work node serves when a work package enters, leaves, or when the work node becomes overloaded.

Creating a work basket

Create a work basket as a discrete, actionable step in your process.

You must define the necessary access control list for this work basket before you can create the work basket.

To create a work basket:

1. On the Definition page, identify and describe the work basket.
 - a. Enter a name for the work basket in the **Name** field.

Tip: Ensure that the name that you use is not also being used as the name of a process. You cannot specify as a subprocess any process that has the same name as a work node.
 - b. Optional: In the **Description** field, enter a description (up to 254 characters). The description that you type here displays in the system administration client when you view details.
 - c. Optional: In the **Long description** field, enter an extended description (up to 2048 characters) of the work basket. This description displays only in the Work Basket Properties and Copy Work Basket windows. You might use this field to indicate where you use this work basket or what dependencies it has so that you don't modify or copy it without considering the ramifications.

- d. In the **Access control list (ACL)** field, select an access control list. Only those that you defined previously are available. The library server checks the ACL for this work node when users want to route work packages from this work node forward and when users want to suspend or resume a work package at this work node.
- e. Optional: In the **Action list** field, select an action list. Only those action lists that you defined previously are available. If you do not specify an action list, your eClient and Client for Windows users will see *only* the named routes (specified as connectors) from this work node.
- f. Optional: In the **Overload limit** field, specify the limit that the work basket cannot exceed. When this limit is reached, the work basket uses the DLL and function that you specify in the **Overload** fields on the Exit Routines page. The exit routine allows additional processing to be performed, such as notifying the process owner. If you do not specify an exit routine, the overload limit has no effect.
- g. Optional: Select the **Set expiration time for completion** check box and use the associated fields to set a period of time. This is the amount of time that a work package can remain at this work node after it arrives at this work node; if the time is exceeded, a notification flag is set. All times are according to Greenwich Mean Time (GMT). After the notification flag is set for a work package, it remains set for the remainder of the process, so any notification flags for remaining work nodes, or for the process as a whole, are moot.

Note, however, that IBM Content Manager does not automatically do anything based on this notification flag. Client for Windows or eClient users can run queries based on the setting of this flag. To use this flag for automatic notification or some other use, you must use the APIs.

- 2. Optional: On the Variables page, specify any variables that the user might need to enter while the work package is at this work basket. You can also specify any variables that you want to display to users at this work basket.

eClient or Client for Windows users see only those variables for which you select **Display to users**. Client users see the value and properties of the variable. The text that you enter in the **Prompt text** field is displayed to users as the label for that variable. If you select **Display to users**, but do not enter any prompt text, users see the variable value and properties without a label, which might be confusing.

Note however, that the settings that you specify here (such as **Display to users**) are enforced by the eClient and Client for Windows, not by the library server. If you create a custom client, you can decide whether to enforce any or all of these settings.

Tip: At this work basket, you can also display to users variables that were set at work nodes earlier in the process. To do this, in the **Variable name** field, type the case-sensitive variable name that you used in the previous work node and select **Display to users**. You can specify different prompt text to display as the label for this variable at this work basket.

For example, when a claim is submitted, the employee who receives the claim at the first work basket might be required to enter certain pertinent data about the customer into the system, such as a customer number. At a subsequent work node, you might want to display the value to the user.

Variables page field name:	Values that you enter at the first work basket:	Values that you enter at a subsequent work node to display the customer number value:
Variable type	Character	Character
Variable name	Customer number	Customer number
Variable length	8	8
Default value		
Display to users	Selected	Selected
Prompt text	Enter the customer number.	Customer number
User input	required	not allowed

You can use variable values to determine which route to take at a decision point later in the process.

3. Optional: On the Exit Routines page, you specify any exit routines that you want to use when entering or leaving this work basket, or when the work basket is overloaded. For each condition:
 - a. Type the path and file name of a DLL that you want to use. The DLL must reside in the same system (not necessarily on the same workstation) as the library server or you get an error. For example, you might enter: `h:\routingapps\wnenter.dll`.
 - b. Type the function name that you want to use as the entry point. You need to define a function for every DLL that you specify, or you get an error. The name of your function must begin with the string `WXV2` to differentiate it from functions that you created prior to IBM Content Manager Version 8 Release 4. The case-sensitive function name that you enter does not require a path or file extension. For example, you might enter: `WXV2wnenter`.

If you specify an exit routine in the **Overload** fields, ensure that you specified an overload limit on the Definition page.

4. Click **OK** to save your work basket. Click **Apply** to save changes and keep the window open. The work basket is identified by name in the graphical builder.

Work basket: A *work basket* is a location at which work waits for action by a user or an application. The action can either be taken on the work waiting at the work basket, or the action could be routing the work to another work node.

Each step in a process corresponds to a real-world task, like verifying a record or rejecting an insurance application. Work baskets contain work packages. A work package contains the location of a document or folder in a database and its priority. A work basket does not perform any actions on the content, rather, it is an indicator of where a work package is in a process. When you assign an access control list (ACL) to a work basket, you give access to users who can perform actions on the work packages contained in that work basket.

A work basket is more than just a virtual basket that has a pile of work stacked in it. You decide what functions a work basket requires to route a work package where it needs to go. You can specify, through dynamic link libraries (DLLs) and functions, what tasks work packages complete upon entering and leaving a work basket. You can also specify a DLL and function to execute when the work basket has reached a limit that you specify.

At a work basket, you can prompt users to enter values or display values that were set at previous work baskets or collection points. In addition to displaying or storing variable values, you can use variable values to determine which route to take at a decision point later in the process.

To define a work basket, you need:

- A name for your work basket
- A predefined ACL

In addition, if you plan to use any DLLs with the work basket, you must know the full directory path for them.

Viewing or modifying a work basket:

To view or modify a work basket:

1. On the Definition page, view or modify the work basket description or properties.

Restriction: You cannot directly change the name of an existing work basket because it might be in use by a process. Instead, you must copy it, rename it, and delete the original work basket.

- a. In the **Description** field, enter or edit the description (up to 254 characters). The description that you type here displays in the system administration client when you view details.
- b. In the **Long description** field, enter or edit the extended description (up to 2048 characters) of the work basket. This description displays only in the Work Basket Properties and Copy Work Basket windows. You might use this field to indicate where you use this work basket or what dependencies it has so that you don't modify or copy it without considering the ramifications.
- c. In the **Access control list (ACL)** field, select an access control list. Only those that you defined previously are available. The library server checks the ACL for this work node when users want to route work packages from this work node forward and when users want to suspend or resume a work package at this work node.
- d. Optional: In the **Action list** field, select an action list. Only those action lists that you defined previously are available. If you do not specify an action list, your eClient and Client for Windows users will see *only* the named routes (specified as connectors) from this work node.
- e. Optional: In the **Overload limit** field, specify the limit that the work basket cannot exceed. When this limit is reached, the work basket uses the DLL and function that you specify in the **Overload** fields on the Exit Routines page. The exit routine allows additional processing to be performed, such as notifying the process owner. If you do not specify an exit routine, the overload limit has no effect.
- f. Optional: Select the **Set expiration time for completion** check box and use the associated fields to set a period of time. This is the amount of time that a work package can remain at this work node after it arrives at this work node; if the time is exceeded, a notification flag is set. All times are according to Greenwich Mean Time (GMT). After the notification flag is set for a work package, it remains set for the remainder of the process, so any notification flags for remaining work nodes, or for the process as a whole, are moot.

Note, however, that IBM Content Manager does not automatically do anything based on this notification flag. Client for Windows or eClient users can run queries based on the setting of this flag. To use this flag for automatic notification or some other use, you must use the APIs.

2. Optional: On the Variables page, specify any variables that the user might need to enter while the work package is at this work basket. You can also specify any variables that you want to display to users at this work basket.

eClient or Client for Windows users see only those variables for which you select **Display to users**. Client users see the value and properties of the variable. The text that you enter in the **Prompt text** field is displayed to users as the label for that variable. If you select **Display to users**, but do not enter any prompt text, users see the variable value and properties without a label, which might be confusing.

Note however, that the settings that you specify here (such as **Display to users**) are enforced by the eClient and Client for Windows, not by the library server. If you create a custom client, you can decide whether to enforce any or all of these settings.

Tip: At this work basket, you can also display to users variables that were set at work nodes earlier in the process. To do this, in the **Variable name** field, type the case-sensitive variable name that you used in the previous work node and select **Display to users**. You can specify different prompt text to display as the label for this variable at this work basket.

For example, when a claim is submitted, the employee who receives the claim at the first work basket might be required to enter certain pertinent data about the customer into the system, such as a customer number. At a subsequent work node, you might want to display the value to the user.

Variables page field name:	Values that you enter at the first work basket:	Values that you enter at a subsequent work node to display the customer number value:
Variable type	Character	Character
Variable name	Customer number	Customer number
Variable length	8	8
Default value		
Display to users	Selected	Selected
Prompt text	Enter the customer number.	Customer number
User input	required	not allowed

You can use variable values to determine which route to take at a decision point later in the process.

3. Optional: On the Exit Routines page, you specify any exit routines that you want to use when entering or leaving this work basket, or when the work basket is overloaded. For each condition:
 - a. Type the path and file name of a DLL that you want to use. The DLL must reside in the same system (not necessarily on the same workstation) as the library server or you get an error. For example, you might enter:
h:\routingapps\wnenter.dll.
 - b. Type the function name that you want to use as the entry point. You need to define a function for every DLL that you specify, or you get an error. The name of your function must begin with the string WXV2 to differentiate it from functions that you created prior to IBM Content Manager Version 8

Release 4. The case-sensitive function name that you enter does not require a path or file extension. For example, you might enter: WXV2wnenter.

If you specify an exit routine in the **Overload** fields, ensure that you specified an overload limit on the Definition page.

4. Click **OK** to save your changes to the work basket. Click **Apply** to save changes and keep the window open.

Copying a work basket:

To copy a work basket, complete the following steps:

1. On the Definition page, identify and describe the new work basket.
 - a. Enter a name for the work basket in the **Name** field.
 - b. Optional: In the **Description** field, enter a description (up to 254 characters). The description that you type here displays in the system administration client when you view details.
 - c. Optional: In the **Long description** field, enter an extended description (up to 2048 characters) of the work basket. This description displays only in the Work Basket Properties and Copy Work Basket windows. You might use this field to indicate where you use this work basket or what dependencies it has so that you don't modify or copy it without considering the ramifications.
 - d. In the **Access control list (ACL)** field, select an access control list. Only those that you defined previously are available. The library server checks the ACL for this work node when users want to route work packages from this work node forward and when users want to suspend or resume a work package at this work node.
 - e. Optional: In the **Action list** field, select an action list. Only those action lists that you defined previously are available. If you do not specify an action list, your eClient and Client for Windows users will see *only* the named routes (specified as connectors) from this work node.
 - f. Optional: In the **Overload limit** field, specify the limit that the work basket cannot exceed. When this limit is reached, the work basket uses the DLL and function that you specify in the **Overload** fields on the Exit Routines page. The exit routine allows additional processing to be performed, such as notifying the process owner. If you do not specify an exit routine, the overload limit has no effect.
 - g. Optional: Select the **Set expiration time for completion** check box and use the associated fields to set a period of time. This is the amount of time that a work package can remain at this work node after it arrives at this work node; if the time is exceeded, a notification flag is set. All times are according to Greenwich Mean Time (GMT). After the notification flag is set for a work package, it remains set for the remainder of the process, so any notification flags for remaining work nodes, or for the process as a whole, are moot.
2. Optional: On the Variables page, specify any variables that the user might need to enter while the work package is at this work basket. You can also specify any variables that you want to display to users at this work basket.

Note, however, that IBM Content Manager does not automatically do anything based on this notification flag. Client for Windows or eClient users can run queries based on the setting of this flag. To use this flag for automatic notification or some other use, you must use the APIs.

2. Optional: On the Variables page, specify any variables that the user might need to enter while the work package is at this work basket. You can also specify any variables that you want to display to users at this work basket.

eClient or Client for Windows users see only those variables for which you select **Display to users**. Client users see the value and properties of the

variable. The text that you enter in the **Prompt text** field is displayed to users as the label for that variable. If you select **Display to users**, but do not enter any prompt text, users see the variable value and properties without a label, which might be confusing.

Note however, that the settings that you specify here (such as **Display to users**) are enforced by the eClient and Client for Windows, not by the library server. If you create a custom client, you can decide whether to enforce any or all of these settings.

Tip: At this work basket, you can also display to users variables that were set at work nodes earlier in the process. To do this, in the **Variable name** field, type the case-sensitive variable name that you used in the previous work node and select **Display to users**. You can specify different prompt text to display as the label for this variable at this work basket.

For example, when a claim is submitted, the employee who receives the claim at the first work basket might be required to enter certain pertinent data about the customer into the system, such as a customer number. At a subsequent work node, you might want to display the value to the user.

Variables page field name:	Values that you enter at the first work basket:	Values that you enter at a subsequent work node to display the customer number value:
Variable type	Character	Character
Variable name	Customer number	Customer number
Variable length	8	8
Default value		
Display to users	Selected	Selected
Prompt text	Enter the customer number.	Customer number
User input	required	not allowed

You can use variable values to determine which route to take at a decision point later in the process.

3. Optional: On the Exit Routines page, you specify any exit routines that you want to use when entering or leaving this work basket, or when the work basket is overloaded. For each condition:
 - a. Type the path and file name of a DLL that you want to use. The DLL must reside in the same system (not necessarily on the same workstation) as the library server or you get an error. For example, you might enter:
h:\routingapps\wnenter.dll.
 - b. Type the function name that you want to use as the entry point. You need to define a function for every DLL that you specify, or you get an error. The name of your function must begin with the string WXV2 to differentiate it from functions that you created prior to IBM Content Manager Version 8 Release 4. The case-sensitive function name that you enter does not require a path or file extension. For example, you might enter: WXV2wnenter.

If you specify an exit routine in the **Overload** fields, ensure that you specified an overload limit on the Definition page.

4. Click **OK** to save your work basket. Click **Apply** to save changes and keep the window open.

Creating a collection point

Create a collection point to collect work before continuing a process.

To define a collection point, you need:

- A name for your collection point
- A predefined ACL
- A list of required item types to complete a folder
- A folder item type that will contain the item types

In addition, if you plan to use any DLLs with the collection point, you must know the full directory path for them.

Recommendation: Keep a list of the item types and work node variables that you use in your process, particularly those that you use in a decision point or a collection point. The library server does not restrict you from deleting item types or work node variables that are used in decision points or collection points.

To define a collection point:

1. On the Definition page, identify and describe the collection point.

- a. Enter a name for the collection point in the **Name** field.

Tip: Ensure that the name that you use is not also being used as the name of a process. You cannot specify as a subprocess any process that has the same name as a work node.

- b. Optional: In the **Description** field, enter a description (up to 254 characters). The description that you type here displays in the system administration client when you view details.
- c. Optional: In the **Long description** field, enter an extended description (up to 2048 characters) of the collection point. This description displays only in the Collection Point Properties and Copy Collection Point windows. You might use this field to indicate where you use this collection point or what dependencies it has so that you don't modify or copy it without considering the ramifications.
- d. In the **Access control list (ACL)** field, select an access control list. Only those that you defined previously are available. The library server checks the ACL for this work node when users want to route work packages from this work node forward and when users want to suspend or resume a work package at this work node.
- e. Optional: In the **Action list** field, select an action list. Only those action lists that you defined previously are available. If you do not specify an action list, your eClient and Client for Windows users will see *only* the named routes (specified as connectors) from this work node.
- f. Optional: In the **Overload limit** field, specify the limit that the collection point cannot exceed. When this limit is reached, the collection point uses the DLL and function that you specify in the **Overload** fields on the Exit Routines page. The exit routine allows additional processing to be performed, such as notifying the process owner. If you do not specify an exit routine, the overload limit has no effect.
- g. Optional: Select the **Set expiration time for completion** check box and use the associated fields to set a period of time. This is the amount of time that a work package can remain at this work node after it arrives at this work node; if the time is exceeded, a notification flag is set. All times are according to Greenwich Mean Time (GMT). After the notification flag is set

for a work package, it remains set for the remainder of the process, so any notification flags for remaining work nodes, or for the process as a whole, are moot.

Note, however, that IBM Content Manager does not automatically do anything based on this notification flag. Client for Windows or eClient users can run queries based on the setting of this flag. To use this flag for automatic notification or some other use, you must use the APIs.

2. Optional: On the Variables page, specify any variables that the user might need to enter while the work package is at this collection point. You can also specify any variables that you want to display to users at this collection point.

eClient or Client for Windows users see only those variables for which you select **Display to users**. Client users see the value and properties of the variable. The text that you enter in the **Prompt text** field is displayed to users as the label for that variable. If you select **Display to users**, but do not enter any prompt text, users see the variable value and properties without a label, which might be confusing.

Note however, that the settings that you specify here (such as **Display to users**) are enforced by the eClient and Client for Windows, not by the library server. If you create a custom client, you can decide whether to enforce any or all of these settings.

Tip: At this collection point, you can also display to users variables that were set at work nodes earlier in the process. To do this, in the **Variable name** field, type the case-sensitive variable name that you used in the previous work node and select **Display to users**. You can specify different prompt text to display as the label for this variable at this collection point.

For example, when a claim is submitted, the employee who receives the claim at the first work node might be required to enter the amount of the claim into the system. At a subsequent work node, you might want to display the claim amount to the user.

Variables page field name:	Values that you enter at the first work node:	Values that you enter at a subsequent work node to display the claim amount value:
Variable type	Integer	Integer
Variable name	ClaimAmount	ClaimAmount
Variable length		
Default value	0	
Display to users	Selected	Selected
Prompt text	Enter the amount of the claim.	Claim amount
User input	required	not allowed

You can use variable values to determine which route to take at a decision point later in the process.

3. Optional: On the Exit Routines page, you specify any exit routines that you want to use when entering or leaving this collection point, or when the collection point is overloaded. For each condition:
 - a. Type the path and file name of a DLL that you want to use. The DLL must reside in the same system (not necessarily on the same workstation) as the library server or you get an error. For example, you might enter:
h:\routingapps\wnenter.dll.

- b. Type the function name that you want to use as the entry point. You need to define a function for every DLL that you specify, or you get an error. The name of your function must begin with the string WXV2 to differentiate it from functions that you created prior to IBM Content Manager Version 8 Release 4. The case-sensitive function name that you enter does not require a path or file extension. For example, you might enter: WXV2wnenter.

If you specify an exit routine in the **Overload** fields, ensure that you specified an overload limit on the Definition page.

Restriction: Although your user exit routine can return a route to the collection point, that route is ignored. Collection points have only one valid route to follow upon completion, which is the route that you designate in the graphical process builder that connects the collection point to the next node in the process.

4. On the Resume List page, identify the items that must arrive at this collection point before the work package can resume moving through the document routing process.
 - a. From the **Folder item type** list, select a folder item type to use to collect documents and folders at this collection point. Folders of other item types or documents flow through the collection point without stopping. If a folder being routed is not one of the folder item types specified in the Resume List, the folder will pass through the collection point and move on to the next work package.
 - b. From the **Required item type** list, select an item type of document or folder that you want to collect at this collection point. When a folder of the item type that you selected in the **Folder item type** field is waiting at this collection point, it collects one or more documents or folders of the item type that you select in the **Required item type** field before work can advance. Documents or folders of other item types flow through the collection point without stopping.
 - c. In the **Quantity needed** field, type the number of **Required item type** items required. For example, an insurance claim might require two damage estimates. When there is only one entry in the resume list for a folder, a value of 0 and 1 both mean that at least one document is required in the folder to satisfy the collection point requirement. When there are multiple entries in the resume list for a folder, the value of 0 and 1 mean different outcomes. For example, Quantity 0 only requires at least one document for one of the required item types whereas Quantity 1 requires at least one document for each required item type.
 - d. Click **Add** to add the required item to the collection point resume list, which is displayed in the table below the entry fields. To remove a required item from the collection point, select the item in the table and click **Remove**.
5. Click **OK** to save your collection point and close the window. Click **Apply** to save your collection point and keep the window open. The collection point is identified by name in the graphical builder.

There is no check interval for the collection point. The library server checks the folder every time a document is added into the folder. The library server performs a check through stored procedure code. A library server monitor is not required for collection point fulfillment checking.

Collection point: A *collection point* is a special work node at which a specified folder waits for arrival of other specified documents or folders. It collects required documents or folders and sends them to another work node when it completes the

list of folder contents. The collection point is designed to accommodate a folder of documents being routed in a process. The library server checks the folder each time a document is added into that folder.

Documents or folders flow through the collection point without stopping if either a folder of the specified type is not waiting at the collection point or, if the documents or folders that reach the collection point are not of the specified type to wait for.

You can specify, through dynamic link libraries (DLLs) and functions, what tasks work packages complete upon entering and leaving a work basket. You can also specify a DLL and function to execute when the work basket has reached a limit that you specify.

At a collection point, you can prompt users to enter values or display values that were set at previous collection points or work baskets. In addition to displaying or storing variable values, you can use variable values to determine which route to take at a decision point later in the process.

To define a collection point, you need:

- A name for your collection point
- A predefined ACL
- A list of required item types to complete a folder
- A folder item type that will contain the item types

In addition, if you plan to use any DLLs with the collection point, you must know the full directory path for them.

A collection point is strictly used in document routing processes. It has nothing to do with resource manager collections.

Viewing or modifying a collection point:

To view or modify a collection point:

1. On the Definition page, identify and describe the collection point.

Restriction: You cannot directly change the name of an existing collection point because it might be in use by another process. Instead, you must copy it, rename it, and delete the original collection point.

- a. In the **Description** field, enter or edit the description (up to 254 characters). The description that you type here displays in the system administration client when you view details.
- b. In the **Long description** field, enter or edit the extended description (up to 2048 characters) of the collection point. This description displays only in the Collection Point Properties and Copy Collection Point windows. You might use this field to indicate where you use this collection point or what dependencies it has so that you don't modify or copy it without considering the ramifications.
- c. In the **Access control list (ACL)** field, select an access control list. Only those that you defined previously are available. The library server checks the ACL for this work node when users want to route work packages from this work node forward and when users want to suspend or resume a work package at this work node.

- d. Optional: In the **Action list** field, select an action list. Only those action lists that you defined previously are available. If you do not specify an action list, your eClient and Client for Windows users will see *only* the named routes (specified as connectors) from this work node.
- e. Optional: In the **Overload limit** field, specify the limit that the work basket cannot exceed. When this limit is reached, the work basket uses the DLL and function that you specify in the **Overload** fields on the Exit Routines page. The exit routine allows additional processing to be performed, such as notifying the process owner. If you do not specify an exit routine, the overload limit has no effect.
- f. Optional: Select the **Set expiration time for completion** check box and use the associated fields to set a period of time. This is the amount of time that a work package can remain at this work node after it arrives at this work node; if the time is exceeded, a notification flag is set. All times are according to Greenwich Mean Time (GMT). After the notification flag is set for a work package, it remains set for the remainder of the process, so any notification flags for remaining work nodes, or for the process as a whole, are moot.

Note, however, that IBM Content Manager does not automatically do anything based on this notification flag. Client for Windows or eClient users can run queries based on the setting of this flag. To use this flag for automatic notification or some other use, you must use the APIs.

2. Optional: On the Variables page, specify any variables that the user might need to enter while the work package is at this collection point. You can also specify any variables that you want to display to users at this collection point.

eClient or Client for Windows users see only those variables for which you select **Display to users**. Client users see the value and properties of the variable. The text that you enter in the **Prompt text** field is displayed to users as the label for that variable. If you select **Display to users**, but do not enter any prompt text, users see the variable value and properties without a label, which might be confusing.

Note however, that the settings that you specify here (such as **Display to users**) are enforced by the eClient and Client for Windows, not by the library server. If you create a custom client, you can decide whether to enforce any or all of these settings.

Tip: At this collection point, you can also display to users variables that were set at work nodes earlier in the process. To do this, in the **Variable name** field, type the case-sensitive variable name that you used in the previous work node and select **Display to users**. You can specify different prompt text to display as the label for this variable at this collection point.

For example, when a claim is submitted, the employee who receives the claim at the first work node might be required to enter the amount of the claim into the system. At a subsequent work node, you might want to display the claim amount to the user.

Variables page field name:	Values that you enter at the first work node:	Values that you enter at a subsequent work node to display the claim amount value:
Variable type	Integer	Integer
Variable name	ClaimAmount	ClaimAmount
Variable length		

Variables page field name:	Values that you enter at the first work node:	Values that you enter at a subsequent work node to display the claim amount value:
Default value	0	
Display to users	Selected	Selected
Prompt text	Enter the amount of the claim.	Claim amount
User input	required	not allowed

You can use variable values to determine which route to take at a decision point later in the process.

3. Optional: On the Exit Routines page, you specify any exit routines that you want to use when entering or leaving this collection point, or when the collection point is overloaded. For each condition:
 - a. Type the path and file name of a DLL that you want to use. The DLL must reside in the same system (not necessarily on the same workstation) as the library server or you get an error. For example, you might enter:
h:\routingapps\wnenter.dll.
 - b. Type the function name that you want to use as the entry point. You need to define a function for every DLL that you specify, or you get an error. The name of your function must begin with the string WXV2 to differentiate it from functions that you created prior to IBM Content Manager Version 8 Release 4. The case-sensitive function name that you enter does not require a path or file extension. For example, you might enter: WXV2wnenter.

If you specify an exit routine in the **Overload** fields, ensure that you specified an overload limit on the Definition page.

Restriction: Although your user exit routine can return a route to the collection point, that route is ignored. Collection points have only one valid route to follow upon completion, which is the route that you designate in the graphical process builder that connects the collection point to the next node in the process.

4. On the Resume List page, identify the items that must arrive at this collection point before the work package can resume moving through the document routing process.
 - a. From the **Folder item type** list, select a folder item type to use to collect documents and folders at this collection point. Folders of other item types or documents flow through the collection point without stopping. If a folder being routed is not one of the folder item types specified in the Resume List, the folder will pass through the collection point and move on to the next work package.
 - b. From the **Required item type** list, select an item type of document or folder that you want to collect at this collection point. When a folder of the item type that you selected in the **Folder item type** field is waiting at this collection point, it collects one or more documents or folders of the item type that you select in the **Required item type** field before work can advance. Documents or folders of other item types flow through the collection point without stopping.
 - c. In the **Quantity needed** field, type the number of **Required item type** items required. For example, an insurance claim might require two damage estimates. When there is only one entry in the resume list for a folder, a value of 0 and 1 both mean that at least one document is required in the

folder to satisfy the collection point requirement. When there are multiple entries in the resume list for a folder, the value of 0 and 1 mean different outcomes. For example, Quantity 0 only requires at least one document for one of the required item types whereas Quantity 1 requires at least one document for each required item type.

- d. Click **Add** to add the required item to the collection point resume list, which is displayed in the table below the entry fields. To remove a required item from the collection point, select the item in the table and click **Remove**.
5. Click **OK** to save your changes to the collection point and close the window. Click **Apply** to save your changes to the collection point and keep the window open.

Copying a collection point:

To copy a collection point, complete the following steps:

1. On the Definition page, identify and describe the collection point.
 - a. Enter a name for the new collection point in the **Name** field.
 - b. Optional: In the **Description** field, enter a description (up to 254 characters). The description that you type here displays in the system administration client when you view details.
 - c. Optional: In the **Long description** field, enter an extended description (up to 2048 characters) of the collection point. This description displays only in the Collection Point Properties and Copy Collection Point windows. You might use this field to indicate where you use this collection point or what dependencies it has so that you don't modify or copy it without considering the ramifications.
 - d. In the **Access control list (ACL)** field, select an access control list. Only those that you defined previously are available. The library server checks the ACL for this work node when users want to route work packages from this work node forward and when users want to suspend or resume a work package at this work node.
 - e. Optional: In the **Action list** field, select an action list. Only those action lists that you defined previously are available. If you do not specify an action list, your eClient and Client for Windows users will see *only* the named routes (specified as connectors) from this work node.
 - f. Optional: In the **Overload limit** field, specify the limit that the collection point cannot exceed. When this limit is reached, the collection point uses the DLL and function that you specify in the **Overload** fields on the Exit Routines page. The exit routine allows additional processing to be performed, such as notifying the process owner. If you do not specify an exit routine, the overload limit has no effect.
 - g. Optional: Select the **Set expiration time for completion** check box and use the associated fields to set a period of time. This is the amount of time that a work package can remain at this work node after it arrives at this work node; if the time is exceeded, a notification flag is set. All times are according to Greenwich Mean Time (GMT). After the notification flag is set for a work package, it remains set for the remainder of the process, so any notification flags for remaining work nodes, or for the process as a whole, are moot.

Note, however, that IBM Content Manager does not automatically do anything based on this notification flag. Client for Windows or eClient users can run queries based on the setting of this flag. To use this flag for automatic notification or some other use, you must use the APIs.

2. Optional: On the Variables page, specify any variables that the user might need to enter while the work package is at this collection point. You can also specify any variables that you want to display to users at this collection point.

eClient or Client for Windows users see only those variables for which you select **Display to users**. Client users see the value and properties of the variable. The text that you enter in the **Prompt text** field is displayed to users as the label for that variable. If you select **Display to users**, but do not enter any prompt text, users see the variable value and properties without a label, which might be confusing.

Note however, that the settings that you specify here (such as **Display to users**) are enforced by the eClient and Client for Windows, not by the library server. If you create a custom client, you can decide whether to enforce any or all of these settings.

Tip: At this collection point, you can also display to users variables that were set at work nodes earlier in the process. To do this, in the **Variable name** field, type the case-sensitive variable name that you used in the previous work node and select **Display to users**. You can specify different prompt text to display as the label for this variable at this collection point.

For example, when a claim is submitted, the employee who receives the claim at the first work node might be required to enter the amount of the claim into the system. At a subsequent work node, you might want to display the claim amount to the user.

Variables page field name:	Values that you enter at the first work node:	Values that you enter at a subsequent work node to display the claim amount value:
Variable type	Integer	Integer
Variable name	ClaimAmount	ClaimAmount
Variable length		
Default value	0	
Display to users	Selected	Selected
Prompt text	Enter the amount of the claim.	Claim amount
User input	required	not allowed

You can use variable values to determine which route to take at a decision point later in the process.

3. Optional: On the Exit Routines page, you specify any exit routines that you want to use when entering or leaving this collection point, or when the collection point is overloaded. For each condition:
 - a. Type the path and file name of a DLL that you want to use. The DLL must reside in the same system (not necessarily on the same workstation) as the library server or you get an error. For example, you might enter:
h:\routingapps\wnenter.dll.
 - b. Type the function name that you want to use as the entry point. You need to define a function for every DLL that you specify, or you get an error. The name of your function must begin with the string WXV2 to differentiate it from functions that you created prior to IBM Content Manager Version 8 Release 4. The case-sensitive function name that you enter does not require a path or file extension. For example, you might enter: WXV2wnenter.

If you specify an exit routine in the **Overload** fields, ensure that you specified an overload limit on the Definition page.

Restriction: Although your user exit routine can return a route to the collection point, that route is ignored. Collection points have only one valid route to follow upon completion, which is the route that you designate in the graphical process builder that connects the collection point to the next node in the process.

4. On the Resume List page, identify the items that must arrive at this collection point before the work package can resume moving through the document routing process.
 - a. From the **Folder item type** list, select a folder item type to use to collect documents and folders at this collection point. Folders of other item types or documents flow through the collection point without stopping. If a folder being routed is not one of the folder item types specified in the Resume List, the folder will pass through the collection point and move on to the next work package.
 - b. From the **Required item type** list, select an item type of document or folder that you want to collect at this collection point. When a folder of the item type that you selected in the **Folder item type** field is waiting at this collection point, it collects one or more documents or folders of the item type that you select in the **Required item type** field before work can advance. Documents or folders of other item types flow through the collection point without stopping.
 - c. In the **Quantity needed** field, type the number of **Required item type** items required. For example, an insurance claim might require two damage estimates. When there is only one entry in the resume list for a folder, a value of 0 and 1 both mean that at least one document is required in the folder to satisfy the collection point requirement. When there are multiple entries in the resume list for a folder, the value of 0 and 1 mean different outcomes. For example, Quantity 0 only requires at least one document for one of the required item types whereas Quantity 1 requires at least one document for each required item type.
 - d. Click **Add** to add the required item to the collection point resume list, which is displayed in the table below the entry fields. To remove a required item from the collection point, select the item in the table and click **Remove**.
5. Click **OK** to save your collection point and close the window. Click **Apply** to save your collection point and keep the window open.

Defining a business application

Identify an external business application to launch from the process.

You must develop and store the external business application as a DLL before you can define it in a work node. The name of the external business application function must begin with the case-sensitive string **WXV2** to differentiate it from external business applications that you wrote prior to IBM Content Manager Version 8 Release 3. The reason for this is that the interface to the user function was changed for Version 8.3, so the library server must be able to differentiate older business applications from Version 8.3 and later business applications so that it knows which parameters to pass.

Your business application can return character values to the document routing process, for example, a claim amount and an approver's name. You can use the business application data structure to pass data (including any work node variable values that the work package carries or the route that it should take upon return)

between the library server and your business application. This data structure is described in the section “Routing a document through a process” in the *Application Programming Guide*.

To define a business application:

1. Enter a name for the business application in the **Name** field.

Tip: Ensure that the name that you use is not also being used as the name of a process. You cannot specify as a subprocess any process that has the same name as a work node.

2. Optional: In the **Description** field, enter a description (up to 254 characters) of the business application. The description that you type here displays in the system administration client when you view details.
3. Optional: In the **Long description** field, enter an extended description (up to 2048 characters) of the business application.
4. In the **Access control list (ACL)** field, select an access control list for the business application node. Only those that you defined previously are available. The library server checks the ACL for this work node when users want to route work packages from this work node forward and when users want to suspend or resume a work package at this work node.
5. In the **Link library name** field, type the fully qualified file and path name of the external business application. For example, you might enter:
c:\routingapps\claimapp.dll.
6. In the **Function name** field, type the name of the function that launches the application. The name of your function must begin with the string WXV2 to differentiate it from functions that you created prior to IBM Content Manager Version 8 Release 4. The function name that you enter does not require a path or file extension. For example, you might enter: WXV2claimapp.
7. Click **OK** to save your business application and close the window. Click **Apply** to save your business application and keep the window open. The business application is identified by name in the graphical builder.

Business application: A *business application node (LOB node)* is a work node that directs work packages to an external business application that you develop. You can also build your application in such a way that it selects the route for the work package to take after the application completes.

The business application node uses an identified function to launch a DLL (Windows) or shared library (AIX, Solaris, or Linux) that runs on the library server or anywhere that the library server can reach using a full path name. You can code the business application to interact with the APIs. You can also code the DLL or shared library to launch other applications, for example, a CICS or IMS program if you have the capability to make such a connection in your system.

For example, if you have an application in place that automatically addresses and prints checks to insurance claimants, you can add a business application work node to your process to send approved claims to that application.

You can use the business application data structure to pass data (including any work node variable values that the work package carries or the route that it should take upon return) between the library server and your business application. This data structure is described in the section “Routing a document through a process” in the *Application Programming Guide*.

To define a business application work node, you need:

- A name for your business application work node
- A predefined ACL
- An existing business application that is a DLL or shared library
- A function that launches the business application

You must know the name of the DLL or shared library and the function that launches it.

Viewing or modifying a business application:

Restriction: You cannot directly change the name of an existing business application because it might be in use by another process. Instead, you must copy it, rename it, and delete the original business application.

To view or modify a business application:

1. In the **Description** field, enter a description (up to 254 characters) of the business application. The description that you type here displays in the system administration client when you view details.
2. In the **Long description** field, enter an extended description (up to 2048 characters) of the business application.
3. In the **Access control list (ACL)** field, select an access control list for the business application node. Only those that you defined previously are available. The library server checks the ACL for this work node when users want to route work packages from this work node forward and when users want to suspend or resume a work package at this work node.
4. In the **Link library name** field, type the fully qualified file and path name of the external business application. For example, you might enter:
c:\routingapps\claimapp.dll.
5. In the **Function name** field, type the name of the function that launches the application. The name of your function must begin with the string WXV2 to differentiate it from functions that you created prior to IBM Content Manager Version 8 Release 4. The function name that you enter does not require a path or file extension. For example, you might enter: WXV2claimapp.
6. Click **OK** to save your changes to the business application and close the window. Click **Apply** to save your changes to the business application and keep the window open.

Copying a business application:

To copy a business application:

1. Enter a name for the business application in the **Name** field.
2. Optional: In the **Description** field, enter a description (up to 254 characters) of the business application. The description that you type here displays in the system administration client when you view details.
3. Optional: In the **Long description** field, enter an extended description (up to 2048 characters) of the business application.
4. In the **Access control list (ACL)** field, select an access control list for the business application node. Only those that you defined previously are available. The library server checks the ACL for this work node when users want to route work packages from this work node forward and when users want to suspend or resume a work package at this work node.

5. In the **Link library name** field, type the fully qualified file and path name of the external business application. For example, you might enter:
c:\routingapps\claimapp.dll.
6. In the **Function name** field, type the name of the function that launches the application. The name of your function must begin with the string WXV2 to differentiate it from functions that you created prior to IBM Content Manager Version 8 Release 4. The function name that you enter does not require a path or file extension. For example, you might enter: WXV2claimapp.
7. Click **OK** to save your changes to the business application and close the window. Click **Apply** to save your changes to the business application and keep the window open.

Deleting a work node

When you delete a work node within the graphical process builder, the work node is only removed from the drawing surface. It is not deleted from the library server.

To delete a work node from the library server:

1. Expand **Document Routing** in the tree view.
2. Click the type of work node that you want to delete (**Work Basket**, **Collection Point**, or **Business Application**) to display the available work nodes of that type in the details pane.
3. In the details pane, right-click the work node that you want to delete and click **Delete**. You can select multiple work nodes to delete by holding down the Ctrl key while you click the work nodes.
4. Click **OK** to confirm the deletion.

Modeling the process graphically

You must launch the graphical process builder to define a new process or modify an existing one. With the graphical process builder, you draw the process with nodes and connectors.

To define document routing processes in IBM Content Manager Version 8.3 and later, you must use the provided graphical process builder.

Restrictions:

- You can continue to run existing processes that were created using Version 8.2 APIs or the Version 8.2 system administration client, but you cannot modify those processes or take advantage of Version 8.3 functionality without using the graphical process builder.
- The processes that you create using the graphical process builder can run only on the Version 8.3 library server.

Accessible process builder: You can create a document routing process in the graphical builder using the keyboard instead of the mouse. Select **Keyboard drawing mode** in the Process Preferences notebook to use the keyboard for drawing.

1. "Defining a new process" on page 295
2. "Adding work nodes as steps in the process" on page 304
3. Optional: "Associating an existing process as a subprocess" on page 305
4. "Connecting steps in a process" on page 306
5. Optional: "Defining a decision point" on page 307

6. "Decision points" on page 309
7. Optional: "Creating parallel routes" on page 310
8. "Parallel routes" on page 310
9. "Verifying the process" on page 311

Defining a new process

When you begin to define a new process, you automatically launch the graphical process builder.

You can define a one-step process, or you can create one process with several steps within it. To create a process:

1. Expand **Document Routing** in the tree view.
2. Right-click **Process** and click **New - Launch Builder**. The Process Properties window opens in front of the graphical builder for modeling the process.
3. Enter a name for the process in the **Name** field.

Restriction: Ensure that the name that you use is not also being used as the name of a work node. You cannot specify as a subprocess any process that has the same name as a work node.

4. Optional: In the **Description** field, enter a description (up to 254 characters) for the process. The description that you type here displays in the system administration client when you view details.
5. Optional: In the **Long description** field, enter an extended description (up to 2048 characters) for the process. This description displays only in the Process Properties and Copy Process windows. You might use this field to indicate how this process relates to others or what dependencies it has. The value in this field can be a reminder so that you do not modify or copy the field without considering the ramifications.
6. In the **Item type access control list (ACL)** field, select an access control list from the list. Only the ACLs that you previously defined are available.
7. Select the **Set expiration time for completion** check box and use the associated fields to set a time period. This is the amount of time that a work package can remain on this process after it starts on the process. If the time is exceeded, a notification flag is set to true. All times are according to Greenwich Mean Time (GMT). After the notification flag is set for a work package, it remains set for the remainder of the process, so any notification flags for remaining work nodes are moot.

Note, however, that IBM Content Manager does not automatically do anything based on this notification flag. Client for Windows or eClient users can run queries based on the setting of this flag. To use this flag for automatic notification or some other use, you must use the APIs.

8. Click **OK** to save your process definition and close the Process Properties window so that you can begin modeling the process in the drawing pane of the graphical builder. Click **Apply** to save changes and keep the Process Properties window open.

Process: A *process* is a series of steps through which work is routed. A process contains at least one start node, one work node, and one stop node. (You can use these one-step processes to create ad hoc processes.) Processes can have as many steps as you want.

A *subprocess* is a process within another process. After you define a process, you can re-use that same process with another process definition. To model a subprocess, use the subprocess node.

You can create a variety of processes.

- You can create serial processes that take work from start to finish through a straight line, without any deviations.
- You can create parallel routes that allow you to direct work through different routes that execute simultaneously. In Figure 23, the FraudCheck and ReviewLargeClaim work nodes are on a parallel route, which begins with the



split node () and ends with the join node ().

Figure 23 shows the XYZ Insurance scenario claims process as modeled in the document routing process builder.

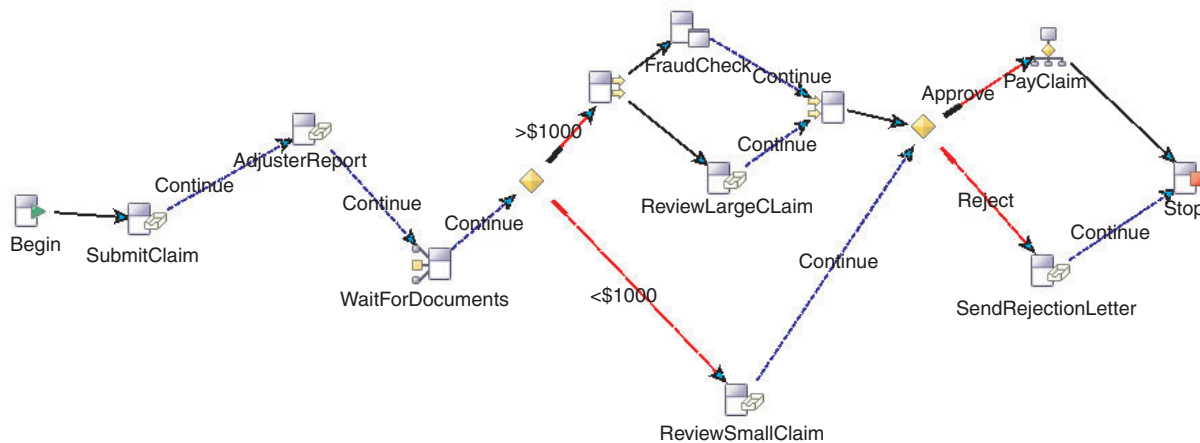


Figure 23. Sample insurance scenario process diagram

Limitations of Version 8.2 and Version 8.3 interoperability:

- To define document routing processes in IBM Content Manager Version 8.3, you must use the provided graphical process builder.
- On a Version 8.3 library server, you can continue to run existing processes that were created using Version 8.2 APIs or the Version 8.2 system administration client, but you cannot modify those processes or take advantage of Version 8.3 functionality without using the graphical process builder.
- Any processes that you create using the graphical process builder, or any Version 8.3 functionality (business application nodes, for example) can run only on the Version 8.3 library server. Furthermore, after you begin using Version 8.3 functionality with your library server, any Version 8.2 clients, including any clients coded using Version 8.2 APIs will not work with the library server until you update them to Version 8.3 level APIs.

Importing a process from XML text:

Open the graphical process builder by opening an existing process or defining a new one. The process you import will be included in this new or existing process.

You can import a process that you previously exported as XML text from the graphical process builder. The primary reason to use this functionality is to move built and verified processes from a test system to a separate production system.

Restriction: You cannot use this functionality to import a process that you exported as XML in the System Administration Client window (for example, by right-clicking a process and clicking **Export All as XML**); this XML text import function works only with files that you previously exported as XML text from the graphical builder. To import an XML file that you exported as XML in the System Administration Client window, you must click **Tools > Import from XML** in the System Administration Client window.

Attention: When a process definition is created by importing the XML text of an exported process definition, the process flow is shown, but the objects do not exist if the process was exported from one library server and imported into another library server. When the process is verified, the verification fails.

To resolve the problem, save the process definition and close the graphical process builder. Create any missing workflow objects (workbasket nodes, collection point nodes, business application nodes, and subprocesses) in the system administration client and then open, verify, and save the process definition.

To import an XML text file that you exported from the graphical builder:

1. Within the graphical process builder, click **File > Import XML text**.
2. Select the XML file that you want to import.
3. Click **Import**. If you selected a file with the same name as a process that currently exists in the library server, a warning displays. If you want to save such an imported diagram, consider using **File > Save As** to give it a different name.
4. Verify the process to determine whether any required objects are missing from this system. Importing an XML text process into the graphical builder does not automatically create the necessary document routing objects (for example, work nodes) for the process.
5. Create necessary document routing objects. You can either create those objects manually, or use the XML export functionality from the System Administration Client window to export them and then import them to the new system.
6. Reverify the process as necessary.
7. Save and close the verified process.

Viewing or modifying a process:

To change a process name, you need to copy it, rename it, and delete the original process. Otherwise, you cannot change a process name, because the process might be in use.

You can update a process at any time, even when a process is in use. Any changes that you make immediately affect the process. For example, if you create a work basket that a work package has not reached yet, then, when the work package arrives at the new work basket, it uses the work basket as if it had always been there. If you add a collection point in a place where the work package has already

passed, the work package will continue on its route. The work package is not affected by any changes to work nodes that it has already passed through.

To view or modify a process:

1. Expand **Document Routing** in the tree view and click **Processes**. The list of existing processes displays in the details pane. Verified processes display with green icons and draft processes display with yellow icons.
2. Right-click an existing process and select **Properties - Launch Builder**. The process opens in the graphical builder.

If you attempt to open a process that you created with a previous version (Version 8.2 or earlier) of the IBM Content Manager system administration client or with the APIs, the following message displays: The process was not created with the graphical builder. The builder will attempt to generate a diagram which will require manual editing and verification. Do you want to continue? If you click **Yes**, the builder renders the diagram, but it collapses all routes into a straight line. You must then move the nodes and possibly remove and replace connectors.

3. To view or modify the process properties:
 - a. Click **Edit > Process Properties**. The Process Properties window opens.
 - b. In the **Description** field, edit or enter a description for the process (up to 254 characters). The description that you type here displays in the system administration client when you view details.
 - c. In the **Long description** field, edit or enter an extended description (up to 2048 characters) for the process. This description displays only in the Process Properties and Copy Process windows. You might use this field to indicate how this process relates to others or what dependencies it has. The value in this field can be a reminder so that you do not modify or copy the field without considering the ramifications.
 - d. In the **Item type access control list (ACL)** field, select an access control list from the list.
 - e. Select the **Set expiration time for completion** check box and use the associated fields to set a time period. This is the amount of time that a work package can remain on this process after it starts on the process. If the time is exceeded, a notification flag is set to true. All times are according to Greenwich Mean Time (GMT). After the notification flag is set for a work package, it remains set for the remainder of the process, so any notification flags for remaining work nodes are moot.

Note, however, that IBM Content Manager does not automatically do anything based on this notification flag. Client for Windows or eClient users can run queries based on the setting of this flag. To use this flag for automatic notification or some other use, you must use the APIs.
 - f. Click **OK** to save your process properties. Click **Apply** to save changes and keep the window open.
4. Modify the diagram as necessary.

Copying a process:

To copy a process:

1. Expand **Document Routing** in the tree view and click **Processes**. The list of existing processes displays in the details pane. Verified processes display with green icons and draft processes display with yellow icons.
2. In the details pane, right-click the process that you want to copy and click **Copy**. The Copy Process window opens.

3. Enter a new name for the process in the **Copy to** field.
4. Click **OK** to save the copy. If this process was not previously verified, a warning message displays, asking whether you want to save this copy as a draft. If you click **No**, the process is not copied.

After the process is copied, it does not immediately display in the Processes list. You must click **View > Refresh** to display the copied process.

Deleting a process:

If you want to delete a process, you must wait until all work packages on the process are complete. You cannot delete a process when it is in use nor can you prevent anyone from starting a process that you want to delete. You cannot determine when a process is in use because you cannot view who is using the process in the system administration client.

- You can attempt to delete the process until the system allows you to delete it.
- You can use the eClient or Client for Windows to view whether there are active work packages on the process that you want to delete.
- You can use the APIs to write a customized program to determine whether there are active work packages on the process that you want to delete.

To delete a process:

1. Expand **Document Routing** in the tree view.
2. Click **Process** to display a list of available processes in the details pane.
3. Right-click the process that you want to delete and click **Delete**. You can select multiple processes to delete by holding down the Ctrl key while you click the processes.
4. Click **OK** to confirm the deletion.

Customizing the display and behavior of the graphical process builder:

When you are modeling your process in the graphical builder, you can change certain characteristics of the display and behavior of the builder.

1. Click **Edit > Process Preferences**. The Process Preferences notebook opens.
2. Modify any of the graphical display characteristics that you want.

To change:	Go to this page:	Select:	Default value:
Icon size	View	Small or Large under Icon size	Large
Whether toolbar text displays	View	Show toolbar text	Cleared
Whether names of nodes display	View	Show text for nodes	Selected

To change:	Go to this page:	Select:	Default value:
Color, type, or size of the connector for alternative paths of work nodes. Each options connector has an associated character strings that describes that option so that users can decide which path to take.	Options connector	<ul style="list-style-type: none"> • A line width and whether the line is solid or broken on the bottom of the page • A color directly from the Swatches page • Numerical values or use the sliders to set values for red, green, and blue saturation on the RGB page 	Blue line of regular, short dashes
Color, type, or size of the connector for expression evaluation routes from decision points. Decision connectors mark routes that are followed based on evaluating expressions in work nodes or the work package; users do not manually decide to follow these routes.	Decision connector	Same as options connector above	Red line of regular, long dashes
Color, type or size of the connector for the main route through the process. Directional connectors mark locations where there are no optional routes and no choices to make, the work must flow along.	Directional connector	Same as options connector above	Solid black line

3. On the Toolbar page, modify any of the graphical builder behavior that you want.

If you want to:	Select or clear:	Default value:
Select a toolbar tool and have it remain selected through multiple uses; the tool remains selected until you click Select .	Select Use sticky tool	Cleared
Select a toolbar tool and have it revert automatically to select mode after use.	Clear Use sticky tool	Cleared
Automatically launch the properties window to create a node when you drop a node into the drawing area.	Select Automatically launch node properties when dropped	Selected

If you want to:	Select or clear:	Default value:
Use the keyboard instead of the mouse to manipulate the diagram.	Select Keyboard drawing mode	Cleared

4. Click **OK** to close the notebook and save the preferences for this process. The preferences are saved with the process, not the builder.

Graphical process builder tools: The graphical process builder is a drawing pane that displays the document routing process diagram as icons and connectors.

Table 65 identifies and describes the tools available in the graphical process builder and the icons that represent them in the drawing pane.

Table 65. Summary of graphical process builder tools


Icon	Description	Example based on an insurance claim process
	<p>A <i>work basket</i> is a location at which work waits for action by a user or an application. The action can either be taken on the work waiting at the work basket, or the action could be routing the work to another work node.</p> <p>A work basket is more than just a virtual basket that has a pile of work stacked in it. You decide what functions a work basket requires to route a work package where it needs to go. You can specify, through dynamic link libraries (DLLs) and functions, what tasks work packages complete upon entering and leaving a work basket. You can also specify a DLL and function to execute when the work basket has reached a limit that you specify.</p>	You might use a work basket to represent the activity of submitting an adjuster report or reviewing a large insurance claim.

Table 65. Summary of graphical process builder tools (continued)











Icon	Description	Example based on an insurance claim process
	<p>A <i>collection point</i> is a special work node at which a specified folder waits for arrival of other specified documents or folders. Documents or folders flow through the collection point without stopping if either a folder of the specified type is not waiting at the collection point or, if the documents or folders that reach the collection point are not of the specified type to wait for.</p> <p>You can specify, through dynamic link libraries (DLLs) and functions, what tasks work packages complete upon entering and leaving a work basket. You can also specify a DLL and function to execute when the work basket has reached a limit that you specify.</p>	<p>You might use a collection point to wait for all of the required documents for a claim (police report and adjuster report, for example) before continuing with the claim process.</p>
	<p>A <i>business application node (LOB node)</i> is a work node that directs work packages to an external business application that you develop. You can also build your application in such a way that it selects the route for the work package to take after the application completes. Values from the document routing process can then be passed to the business application, and control values from the business application can be passed back to the process.</p>	<p>You might have a business application that runs a fraud check against policy holders who have submitted large claims.</p>
	<p>A decision point directs work packages to different work nodes depending on:</p> <ul style="list-style-type: none"> • Information that users provide • Work package properties • Attribute values for the routed items 	<p>You might use a decision point to send the insurance claim through different routes in your process depending on whether it is approved or rejected.</p>
	<p>A subprocess is a predefined document routing process that you want to incorporate into this process. You must ensure that this subprocess can correctly process the data that you send it, for example, will decision points in the subprocess work predictably with the work package from the main process?</p> <p>Restriction: You cannot specify as a subprocess any process that has the same name as a work node.</p>	<p>You might have a separate business process that includes the required steps for paying approved claims. This process is a separately defined process that you can include in the insurance claim process with a subprocess node and in other applicable processes as necessary.</p>

Table 65. Summary of graphical process builder tools (continued)

Icon	Description	Example based on an insurance claim process
	Marks the beginning of a parallel route. The split node is a virtual node in that no activity is performed there. Each split node must have a corresponding join node.	You might want to run a fraud check at the same time that the underwriter is reviewing the claim. You use a split node to send work to the underwriter using a workbasket and to the fraud check business application.
	Marks the end of a parallel route. The join node is a virtual node in that no activity is performed there. Each join node must have a corresponding split node.	You might use a join node to reconnect the process after the underwriter reviews the claim in the workbasket and after the fraud check business application completes.
	A start node begins the document routing process. The process diagram must have only one start node. The start node is a virtual node in that no activity is performed there.	—
	A stop node ends the process. Every document routing process diagram contains at least one stop node. The stop node is a virtual node in that no activity is performed there.	—
	A comment is any additional explanation that you want to add to the process diagram that does not fit in the names that you give to various nodes and connectors. Comments display only in the process diagram; client users do not see these comments.	—
	A connector connects the work nodes and virtual nodes to define the process flow.	—

You can view the names of the tools by opening the Process Preferences (clicking **Edit > Process Preferences**) and selecting **Show toolbar text** on the View page.

Keyboard input and navigation for process builder:

To use the keyboard instead of the mouse in the graphical process builder, click **Edit > Process Preferences** and select **Keyboard drawing mode**.

Use the following keys to navigate in the builder and draw the process diagram:

F10 Navigates to the menu bar.

F6 Navigates to the drawing surface.

Left Arrow

Scrolls to the left.

Right Arrow

Scrolls to the right.

Up Arrow

Scrolls up.

Down Arrow

Scrolls down.

Ctrl+Enter

Based on the selection from the **Tools** menu, drops a new node or connector on the drawing surface. You are prompted for where to place the new node in relation to other nodes on the drawing surface.

Shift+Enter

Cycles the selection of connectors and nodes that are on the drawing surface.

Enter Opens properties for the selected node or connector.

Delete Deletes the selected node or connector

Virtual node: A *virtual node* is a distinguishable point within your process diagram at which no work is performed, but which is required to effectively render the process flow. From the perspective of the client applications, work flows through the virtual nodes. All of the following nodes are virtual nodes:

- Start
- Stop
- Split
- Join
- Decision point
- Subprocess

Virtual nodes are represented by specific icons in your process diagram.

Every diagram must have one start node and at least one stop node. (Note that if you add multiple stop nodes, they act as a single stop node.)

For each split node, you must include a corresponding join node. When work reaches a split node, it copies itself to follow the parallel routes until it encounters a join node where it can combine again.

Diagrams can have multiple split node and join node pairs. If you nest split node and join node pairs, the nesting behaves the way parentheses behave in mathematical equations in that the innermost split node corresponds to the innermost join node.

Adding work nodes as steps in the process

In the builder, begin to model your process by adding new or existing work nodes to the process.

In the graphical process builder, you can graphically create or update your process. When you are creating a process, the builder supplies the start node and end node for you.

You can add a work node to a process at any time. You might update a process because the way an enterprise performed a process has changed or no longer exists.

1. Select the type of work node that you want to add to your process.
 - In the toolbar, click the icon for the work node.
 - Select the work node from the **Tools** menu.
2. Click in the builder area where you want to add the work node. A work node icon displays in the builder and the New Work Basket, New Collection Point, or New Business Application window opens.
3. Select an existing work node or specify properties to create one.
 - Select an existing work node from the **Name** list. The remaining fields are completed with the previously specified values, which you cannot change from inside the builder. Click **OK** to save the work node.
 - “Creating a work basket” on page 276
 - “Creating a collection point” on page 283
 - “Defining a business application” on page 291

If you click **Cancel**, the window closes and does not save the information, but the node appears as a modelled node with a default name. If you do not want the node name to appear, you can select it and click **Delete**.

You can continue modifying the process in the builder.

- You can add work nodes by repeating this task.

Restriction: Although you can reuse work nodes in different processes, you can include only one instance of a specific work node in a process.

- You can move nodes by dragging and dropping them. If you want to move a work node to a different point in a process, you must first delete any connectors to and from it, otherwise, when you drag the work node, the connectors remain attached to it. After you remove the existing connectors, you can move the work node to the new location and establish new connections at its new location.
- You can delete a work node by clicking it and pressing Delete.

Work step: A *work step* is a discrete point in a document routing process through which an individual work package must pass. A work step most often corresponds to a work node, but might also be a decision point.

Ad hoc routing process: You can use an *ad hoc routing process* to remove a document or folder from one process and put it in another.

An ad hoc routing process consists of a single step; you can use a series of such processes to direct work from one process to another process.

For an ad hoc routing process, you need at least one work node in the graphical builder. **Start** and **End** are virtual nodes. They indicate only that a process has started or ended. If you try to save a new process with only these two labels, you get an error.

Associating an existing process as a subprocess

Optional: Any existing process can become a subprocess of your new process.

A subprocess is an existing, working process. Before you can add a subprocess, you must create the process that you want to add.

You must ensure that the subprocess that you add can correctly process the data that you send it. For example, will decision points in the subprocess work predictably with the work package from the main process?

To add a subprocess:

1. Select the subprocess tool.
 - In the toolbar, click the **Subprocess** icon.
 - Click **Tools > Subprocess**.
2. Click in the builder area where you want to add the subprocess. A subprocess icon displays in the builder and the Subprocess Definition window opens.
3. In the **Name** field, select a previously defined process.

Restriction: Any previously defined processes that have the same name as an existing work node are not listed.

The remaining fields are populated with the properties of the selected process and greyed out so that you cannot change them.

4. Click **OK** to add the process as a subprocess.

During execution, when a work package reaches a subprocess node, it copies itself to execute the subprocess until it returns to the main process where it can combine again. In practice, this means that any work node variables or properties associated with the work package or the data that it contains are carried with the work package instance as the subprocess executes. During subprocess execution, any updates to the work package instance are mirrored in the work package instance in the main process.

Connecting steps in a process

Connect the start node, work nodes, decision points, any split and join nodes, and the end node to define the process flow.

You must create the two nodes that you want to connect before you can connect them.

1. Select the connector tool.
 - In the toolbar, click the **Connector** icon.
 - Click **Tools > Connector**.
2. Click an existing node in the builder that you want to be the source of the connection.
3. Click an existing node in the builder that you want to be the target of the connection. An arrow displays, pointing from the node that you specified as the source toward the node that you specified as the target.

The connector displays differently depending on what type of connection is being made (directional, optional, or decision). You can set the appearance of these different connectors in the Process Preferences notebook, but you are not required to remember or know when to apply these different connectors; they are applied automatically based on the context.

4. Identify the connector.
 - a. Double-click the arrow to open the Connection window.
 - b. In the **Name** field, type a name for the connection or select an existing name. If your company is using the Client for Windows or the eClient, this name displays, exactly as you type it, as a menu choice in the clients. The default route name is Continue.
 - c. Click **OK** to close the window. The connector name displays in the builder.

Work packages flow through the process following the connections that you create.

Defining a decision point

Optional: Define decision points if you want to automatically and conditionally branch your process based on document attributes, work package properties, or work node variables.

During the process, users might respond to prompts or change document or folder attributes. You can create a decision point that directs work packages to different work nodes depending on the information that users provide during the process or on attribute values or properties of the data flowing through the process. For example, you might want an insurance claim to go into one work basket if the claimant's last name begins with A through M, and to another work basket if it begins with N through Z. Then, when the user who enters the claimant's name sends the work package to the next work basket, the work package routes automatically to the appropriate work basket.

Important: If the expression defined for the decision point uses item type attributes, then you might need to create one component index for each attribute used in the predicate. Creating component indexes enables the database manager to use index scans on the component tables instead of table scans. The use of index scans can improve performance when the expression is evaluated at runtime. For small component tables of 10 rows or fewer, no indexes are needed.

Recommendation: Keep a list of the item types and work node variables that you use in your process, particularly those that you use in a decision point or a collection point. The library server does not restrict you from deleting item types or work node variables that are used in decision points or collection points.

1. Select the decision point tool.
 - In the toolbar, click the **Decision Point** icon.
 - Click **Tools > Decision Point**.
2. Click in the builder where you want to add the decision point. A decision point icon displays in the builder.
3. If you have not done so, define the work nodes that will receive the work packages from this decision point.
4. Define a connection from the decision point to each of the possible work nodes. For each connection, a red arrow pointing from the decision point to the work node displays.
5. Double-click the connector between the decision point and one of the work nodes. Although you can double-click other nodes to open their properties, with the decision point, you must double-click the connector. This is because the decision point can have multiple routes, and each route requires its own definition. The Decision Point window opens.
6. In the **Name** field, provide a short name for this route. This name displays next to the connector in the builder.
7. Optional: Describe the route in the **Description** field (up to 254 characters).
8. Identify the route type.

Requirement: Each decision point must have at least one route to follow if all expression evaluation routes are false. To specify this route, click **Otherwise route**.

9. Define an expression. If you selected **Otherwise route**, skip this step.
 - a. Identify what the expression will evaluate.

Select this radio button:	To evaluate:
Work node variables	The variable values specified at previous work baskets or collection points, including prompted user responses.
Work package properties	The properties of the work package, such as the status or whether the notification flag is set.
Item type attributes	The current attributes of the document or folder routed by the work package; the current version of the document or folder is evaluated.

b. Create the expression.

If you selected this radio button:	Create the expression ¹ :
Work node variables	<ol style="list-style-type: none"> 1. Select a work node variable to evaluate from the Variable list, and then an operator and value to evaluate the variable against. For example, approval status = Y. Tip: The Variable list is not case-sensitive and does not display duplicates. 2. Click Add to add the expression to the Expression field.
Work package properties	<ol style="list-style-type: none"> 1. Select a work package property to evaluate from the Property list, and then an operator and value to evaluate the property against. For example, Owner = jsmith. 2. Click Add to add the expression to the Expression field.
Item type attributes	<ol style="list-style-type: none"> 1. Select the item type to evaluate from the Item type list. For example, Claims. 2. Select an attribute to evaluate from the Attribute list (for example, LastName), and then an operator and value to evaluate the attribute against. For example, LastName = Smith. 3. Click Add to add the expression to the Expression field. In this example, Claims.LastName = Smith displays.

If you selected this radio button:

Create the expression¹:

Notes:

1. **Restriction:** For both workstation and z/OS based library servers, the length of the SQL expression is limited to 16000 bytes. For a library server on Oracle, the length of the SQL expression is limited to 32768 bytes.
2. The value of a workflow variable is physically stored as a character string with a maximum length of 254, even though the variable definition in a work node is defined as INTEGER type. The type in the variable definition is to serve as an interpretation of variable type for clients and applications.
3. If you have duplicate work node names, only the first one found (starting at the decision point node and traversing back towards the start node) is displayed in the **Variable** list.
4. If you have work nodes with the same work node variable name but are different types and all of the work nodes out-bound connector connects to the same decision point node, only the first one connected to the decision point node is displayed in the **Variable** list.
5. If an item type or attribute was recently added or deleted, you might need to save the current process, re-open the process, and click the **Item type attributes** radio button to see it listed.

Use the push buttons to insert operators or parentheses so that you can combine multiple conditions in the expression.

- c. Click **Verify expression** to test the SQL expression.
 - d. If you have more than one expression evaluation route for this decision point, you can set the precedence for the routes on the Precedence page. The Precedence page displays only when you have defined more than one expression evaluation route for a decision point. At run time, the expressions are evaluated in order of precedence. The route for the first expression that is true is followed. If all of the expressions are false, then the otherwise route is followed.
10. Click **OK** to save this decision point route and close the window.

Decision points

A decision point is an *unstaffed* work node in the process that chooses one of several possible routes that the work package proceeds through.

You can use work node variables, work package properties, or user defined attributes of item types to define the decision point.

Whenever a work package reaches a decision point, IBM Content Manager tests the work package for decision expressions that are associated with the routes. These routes are tested in the order of their assigned precedence, for example: 1, 2, 3. The work package continues down the first expression that returns a value of true.

When you define a decision point, you must specify an *otherwise route*, which is one route for the work package to follow if all expression evaluation routes are false. An otherwise route has a precedence value of 0. A work package cannot be sent down more than one route.

When you model a decision point node, be sure to correctly define all of the nodes before the decision point. If you do not, then a decision might be made on the work node variables that are defined in workbaskets, collection points, and subprocess nodes (where workbaskets and collection points are part of the process) that cannot be reached before the decision point.

When the user displays the decision branch, it lists all of the work node variables for which the decision point can be defined. This list accumulates the variables as the work package traverses from the start node to each connected node prior to the decision point node.

Important: An error can occur if the decision point node cannot read the work node variables that it needs, for example, from a workbasket, collection point, or subprocess. The following two scenarios can cause this to happen:

- Updating or deleting a workbasket, collection point, or subprocess without updating or deleting its corresponding decision in the decision point node.
- Defining a decision that is based on work node variables that were not assigned yet. For example, the work package might skip over certain nodes because of branching or parallel routing.

Creating parallel routes

Optional: Use split-join node pairs to create parallel routes in your process.

Requirement: Each split node must have a corresponding join node.

Diagrams can have multiple split node and join node pairs. If you nest split node and join node pairs, the nesting behaves the way parentheses behave in mathematical equations in that the innermost split node corresponds to the innermost join node.

To create a parallel route:

1. Select the split node.
 - In the toolbar, click the **Split** icon.
 - Click **Tools > Split**.
2. Click in the builder area where you want to split the process.
3. Select the join node.
 - In the toolbar, click the **Join** icon.
 - Click **Tools > Join**.
4. Add any work nodes, decision points, or subprocesses that you want to execute within each parallel route. You can also add additional split-join node pairs.
5. Click in the builder area where you want to join the process.
6. Using the connector tool, connect the main process and parallel routes.
 - a. Connect the main process to the split node.
 - b. Connect the split node to the first node on each parallel route.
 - c. Along each of the parallel routes, connect the nodes.
 - d. Connect the last node on each of the parallel routes to the join node.

During execution, when a work package reaches a split node, it copies itself to follow the parallel routes until it encounters a join node where it can combine again. In practice, this means that any work node variables or properties associated with the work package or the data that it contains are carried with each work package instance as it follows each parallel route. Any updates to a work package instance on one route are mirrored in the work package instance on the other route.

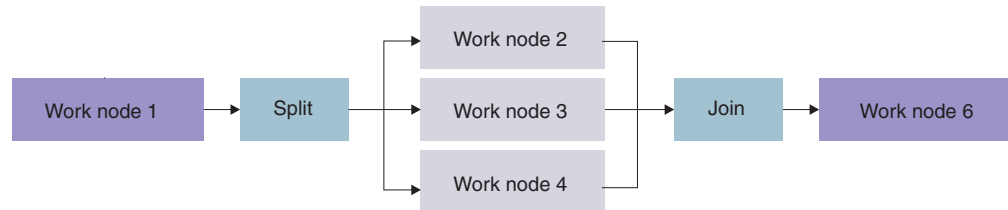
Parallel routes

You can replicate a work package into multiple linked copies and forward them into parallel routes.

Creating parallel routes forms a *split-join enclosure* that starts with a split node and ends with a join node, enclosing the parallel routes that is similar to parentheses in a mathematical expression. The mapping is one-to-one: A split-join enclosure always starts with a split node and ends with a join node. You can create nested parallel routes.

Example

The following example shows a work package that is replicated into three parallel routes.



In the example, the work package moves through the process as follows:

1. The work package leaves work node 1. The split node routes the package to multiple work nodes (2, 3, and 4).
2. If the work package is updated in work node 2, work node 3, or work node 4, then all three copies mirror the same update.
3. Later in the process, the work package joins together at a single join node before continuing to the next work node (work node 6).

Do not connect routes that breach the split-join enclosure. For example, you cannot connect a route between work node 4 and work node 6 because that will breach the split-join enclosure. However, you can connect a direct route between work node 2 and work node 3 because those nodes are within the split-join enclosure.

Verifying the process

Run the verification process to ensure that the process that you modeled matches the data in your system.

You can verify your process at any time by completing the following steps:

1. Click **File > Verify**. The Verify window opens.
2. Review the **Verification results** list for errors or success. If you have errors, complete the following steps:

Requirement:

- a. If you need additional information about an error message, click the message. The associated incorrect action item or connector is highlighted in the diagram. If you select the error message and click **Help**, more information about the error displays, if it is available.

Note that not all the messages listed in the **Verification results** list prevent the workflow process diagram from being verified successfully. Some messages are simply warnings.

- b. Correct any errors.
 - c. Click **Reverify** to ensure that there are no more errors.
3. Click **Close** to close the window. If you click **Close** in while the verification process is running, the process verification stops and the window closes.

When you view the list of existing processes in the details pane of the system administration client, verified processes display with green icons and draft processes display with yellow icons.

Printing the process diagram

Before you can print a process diagram, you must have it open in the graphical process builder.

You can print a process diagram at any time from the graphical process builder.

1. Click **File > Print Diagram**. A standard Print window opens.
2. Specify the location and options for printing the diagram.
3. Click **OK**.

Exporting a process as XML text

Before you can export a process as XML, you must create and verify it in the graphical process builder. The verification process does not have to complete successfully before you can export the process. To export a previously created and verified process, you must first open it in the graphical process builder.

You can export a new process that you have open in the builder or an existing process. The primary reason to use this functionality is to move built and verified processes from a test system to a separate production system.

Do not confuse this functionality with the XML export functionality that is available from the System Administration Client window--that XML export function exports a full range of system administration data as binary XML, this XML export function exports only the content of the graphical builder as XML text for import within the graphical builder on another system.

Although you are exporting the content of the graphical builder, you are *not* exporting the definition of the included document routing objects (for example, work nodes). If the necessary document routing objects do not exist on the target system, you can use the XML export functionality from the System Administration Client window to export them.

To export a process from the graphical builder as XML text:

1. Within the graphical process builder, click **File > Export XML text**.
2. Specify a name and location for the exported XML file.
3. Click **Export**.

The file is exported as a XML text file.

Creating a worklist

You create worklists to filter user access to work packages at specified work nodes.

Before you can create a worklist, you must first create the access control list that you want to use for it and the work nodes that you want to associate with it.

To create a worklist:

1. Expand **Document Routing** in the tree view.
2. Right-click **Worklist** and click **New**. The New Worklist window opens.
3. On the Definition page, identify and define the properties for the worklist.

- a. Type a name for the worklist in the **Name** field.
- b. Optional: In the **Description** field, enter a description (up to 254 characters) for the worklist. The description that you type here displays in the system administration client when you view details.
- c. From the **Item type access control list (ACL)** field, select an access control list. Only the ACLs that you defined previously display.
- d. Optional: You can specify how many work packages to display to your user in the worklist. If you decide not to modify any of the default selections, the worklist returns all work packages that a user has access to based on priority.

Select the order to display the work packages in the worklist:

By priority

Work packages are sorted by priority.

By date

Work packages are sorted in ascending order by the last update time of the work package.

Select the number of work packages that are routing documents or folders to which the user has access. These work packages must originate from work nodes that you include in the worklist (on the Nodes page) and must match the filter criteria that you select:

One Returns one work package at a time.

All Returns all work packages that meet criteria.

Maximum

Limits the number of work packages returned. You must specify the limit in the field provided.

Select one or more methods to filter the worklist:

Filter on notify state

Activates the choice of whether you want the user to see work packages that are in notify state or not in notify state.

Filter on suspend state

Activates the choice of whether you want the user to see work packages that are in suspend state or not in suspend state.

Filter on owner

Filters the work packages by owner.

4. On the Nodes page, you populate and prioritize the worklist. Press Ctrl and click to select more than one work node at a time.

a. Populate the worklist.

- Add a selected work node from the **Select available nodes list** to the **Prioritize nodes in worklist** list by clicking **Add**.
- Remove an action from the **Prioritize nodes in worklist** list to the **Select available nodes** list by clicking **Remove**.
- By default the **Select available nodes list** is populated with all work nodes that are available on the system, but you can click **Work basket**, **Collection point**, or **Business application** to view only those types of work nodes.
- Use the search fields to search for nodes to add to or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.

- b. Use the **Move Up** and **Move Down** push buttons to prioritize the work nodes in the **Prioritize nodes in worklist** list. Because the worklist can include work nodes from multiple processes, prioritizing the nodes can help clarify the urgency of work across processes.
5. When you finish creating the new worklist, click **OK** or **Apply**.

Worklist

A *worklist* filters work packages that are associated with one or more specified work nodes.

You define a worklist to filter work packages that are available to your users. From the Client for Windows, eClient, or a custom client, your users access the document routing process from the worklist. Users complete required activities (which you defined with the work nodes in the process) for work packages and move work packages through your process. The activities that your users perform, combined with the criteria and properties that you defined for your process, move work through the process.

A worklist spans all work nodes, regardless of process. Work packages are prioritized in the worklist based on the priority of the work nodes specified in the list and on other criteria that you select, such as priority or work package creation date.

You need to assign work nodes to a worklist and give the worklist an access control list (ACL). The ACL of the worklist filters the users who can access that worklist. The ACLs of the data routed in the work packages further restrict access to the work packages listed in the worklist. For example, an insurance underwriter and an underwriter assistant can have access to the same worklist, but, based on their privileges and the ACL of the data in the work packages, the underwriter sees a different list of work packages than the underwriter assistant.

Work package

A *work package* contains the information that a user needs to complete a task. The user is unaware of a work package because the user works on the item it references, not on the work package itself. Work package properties include a set of information about the item or items being routed such as, item ID, author, process, step, priority, status, and timestamps for last change, notification, and resumption. IBM Content Manager supports a complex process, allowing you to create processes that determine what route a work package takes based on the actions or non-actions of users or applications.

You do not create work packages. Work packages are created by the system with information from the user who starts a process. During the process:

- Users can update work package properties and supply work node variables if they have the `ItemUpdateWork` privilege and are included in the ACL for the corresponding work node.
- Users can retrieve work packages at specific work nodes if they have the `ItemGetWork` privilege and are included in the ACL of the item that is contained in the work package.
- Users can route a work package from one work node to another if they have the `ItemRoute` privilege and are included in the ACL for the source work node.

The user that starts an item on a process is the owner of the work package that the item is in. During the process, you can modify the owner of a work package by modifying the work package attributes.

For more information about starting a process, see the eClient or Client for Windows information.

Viewing or modifying a worklist

To view or modify a worklist:

1. Expand **Document Routing** in the tree view.
2. Click **Worklist**, right-click on an existing worklist and select **Properties**. The Worklist Properties window opens.
3. On the Definition page, identify and define the properties for the worklist.

Restriction: You cannot directly change the name of an existing worklist because it might be in use. To change a worklist name, you must copy it, rename it, and delete the existing worklist.

- a. Optional: In the **Description** field, enter a description (up to 254 characters) for the worklist. The description that you type here displays in the system administration client when you view details.
- b. From the **Item type access control list (ACL)** field, select an access control list. Only the ACLs that you defined previously display.
- c. Optional: You can specify how many work packages to display to your user in the worklist. If you decide not to modify any of the default selections, the worklist returns all work packages that a user has access to based on priority.

Select the order to display the work packages in the worklist:

By priority

Work packages are sorted by priority.

By date

Work packages are sorted in ascending order by the last update time of the work package.

Select the number of work packages that are routing documents or folders to which the user has access. These work packages must originate from work nodes that you include in the worklist (on the Nodes page) and must match the filter criteria that you select:

One Returns one work package at a time.

All Returns all work packages that meet criteria.

Maximum

Limits the number of work packages returned. You must specify the limit in the field provided.

Select one or more methods to filter the worklist:

Filter on notify state

Activates the choice of whether you want the user to see work packages that are in notify state or not in notify state.

Filter on suspend state

Activates the choice of whether you want the user to see work packages that are in suspend state or not in suspend state.

Filter on owner

Filters the work packages by owner.

4. On the Nodes page, you populate and prioritize the worklist. Press Ctrl and click to select more than one work node at a time.

- a. Populate the worklist:
 - Add a selected work node from the **Select available nodes list** to the **Prioritize nodes in worklist** list by clicking **Add**.
 - Remove an action from the **Prioritize nodes in worklist** list to the **Select available nodes** list by clicking **Remove**.
 - By default the **Select available nodes list** is populated with all work nodes that are available on the system, but you can click **Work basket**, **Collection point**, or **Business application** to view only those types of work nodes.
 - Use the search fields to search for nodes to add to or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
 - b. Use the **Move Up** and **Move Down** push buttons to prioritize the work nodes in the **Prioritize nodes in worklist** list. Because the worklist can include work nodes from multiple processes, prioritizing the nodes can help clarify the urgency of work across processes.
5. When you finish modifying the worklist, click **OK** or **Apply**.

Copying a worklist

To copy a worklist:

1. Expand **Document Routing** in the tree view.
2. Click **Worklist**, right-click an existing worklist and click **Copy**. The Copy Worklist window opens.
3. On the Definition page, identify and define the properties for the worklist.
 - a. Type a new name for the worklist in the **Name** field.
 - b. Optional: In the **Description** field, enter a description (up to 254 characters) for the worklist. The description that you type here displays in the system administration client when you view details.
 - c. From the **Item type access control list (ACL)** field, select an access control list. Only the ACLs that you defined previously display.
 - d. Optional: You can specify how many work packages to display to your user in the worklist. If you decide not to modify any of the default selections, the worklist returns all work packages that a user has access to based on priority.

Select the order to display the work packages in the worklist:

By priority

Work packages are sorted by priority.

By date

Work packages are sorted in ascending order by the last update time of the work package.

Select the number of work packages that are routing documents or folders to which the user has access. These work packages must originate from work nodes that you include in the worklist (on the Nodes page) and must match the filter criteria that you select:

One Returns one work package at a time.

All Returns all work packages that meet criteria.

Maximum

Limits the number of work packages returned. You must specify the limit in the field provided.

Select one or more methods to filter the worklist:

Filter on notify state

Activates the choice of whether you want the user to see work packages that are in notify state or not in notify state.

Filter on suspend state

Activates the choice of whether you want the user to see work packages that are in suspend state or not in suspend state.

Filter on owner

Filters the work packages by owner.

4. On the Nodes page, you populate and prioritize the worklist. Press Ctrl and click to select more than one work node at a time.
 - a. Populate the worklist:
 - Add a selected work node from the **Select available nodes list** to the **Prioritize nodes in worklist** list by clicking **Add**.
 - Remove an action from the **Prioritize nodes in worklist** list to the **Select available nodes** list by clicking **Remove**.
 - By default the **Select available nodes list** is populated with all work nodes that are available on the system, but you can click **Work basket**, **Collection point**, or **Business application** to view only those types of work nodes.
 - Use the search fields to search for nodes to add to or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
 - b. Use the **Move Up** and **Move Down** push buttons to prioritize the work nodes in the **Prioritize nodes in worklist** list. Because the worklist can include work nodes from multiple processes, prioritizing the nodes can help clarify the urgency of work across processes.
5. When you finish creating the new worklist, click **OK** or **Apply**.

Deleting a worklist

To delete a worklist:

1. Expand **Document Routing** in the tree view.
2. Click **Worklist** to display the available worklists in the details pane.
3. Right-click the worklist that you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

Establishing automatic workflow

Optional: After you create a process, establish automatic workflow so that new items can start on the process when they are created.

Before you can establish automatic workflow, you must create the document routing process through which you want items to run.

You can use automatic workflow to start all items of a particular item type on a document routing process as soon as they are created in the system. To automatically start an item of a particular item type on a previously defined document routing process:

1. Create or modify the item type for which you want to establish automatic workflow. For a new item type, in the tree view of the System Administration Client window, right-click **Item Types** and click **New**. For an existing item type, right-click the existing item type and click **Properties**. The New Item Type Definition or Item Type Properties window opens.
2. On the Definition page, select a document routing process in the **Start item on process field**.
3. Optional: If you specify the same process for two different item types, you can type an integer in the **Priority** field to indicate which of them receives a higher priority.
4. Click **OK** to save the definition and close the window.

Any new items that are created using this item type are started on the specified document routing process automatically.

Related tasks

“Creating an item type” on page 153

Managing object storage in IBM Content Manager

The resource manager is the component of IBM Content Manager that manages objects. Managing object storage consists of creating the collections that organize the objects in your system and creating the additional entities that support the collections. This section explains how to store objects, create collections, and migrate objects.

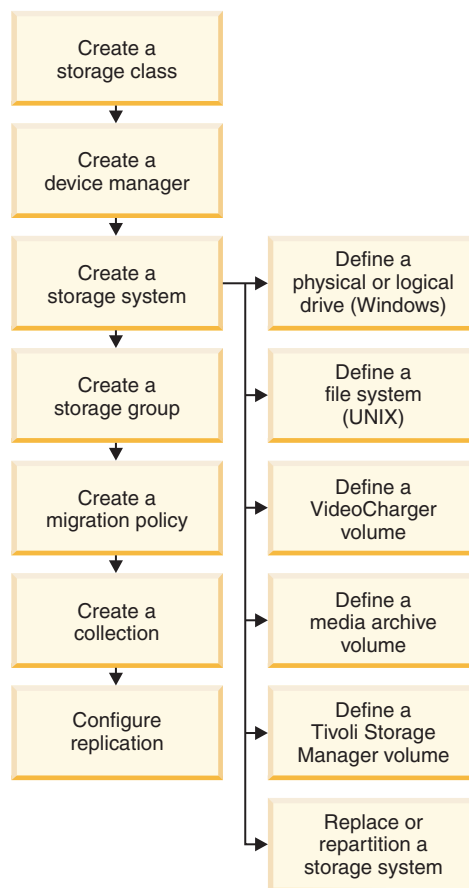


Figure 24. Common tasks relating to managing object storage and how they relate to each other.

To set up storage, complete the following tasks:

1. Create a storage class.
2. Create a device manager.
3. Create a storage system. You can create different types of storage systems:

File systems

You can set up file system volumes or network-attached storage on UNIX and Windows resource managers.

DB2 Content Manager VideoCharger

You can set up DB2 Content Manager VideoCharger and media archive volumes.

Tivoli Storage Manager

You can set up Tivoli Storage Manager volumes with or without retention protection.

4. Create a storage group
5. Configure migration.
6. Create a collection.
7. Configure replication.

“Creating a storage system” on page 329

Object storage

Attention: For information about how to create storage classes, management classes, storage groups, and OAM collections in the z/OS environment, see IBM *z/OS: Object Access Method Planning, Installation, and Storage Administration Guide for Object Support* (SC35-0426).

With Content Manager EE you can store multiple copies of objects and migrate them from one storage location to another. You plan which objects to replicate or migrate at the time that you store the object.

When you manage object storage, you create the collections that organize the items in your system and you create the migration policies that move those items from one type of storage to another. A *collection* identifies a group of items.

Other tasks included in managing object storage are determining which media to use to store the items and identifying the schedule for moving the items from one media type to another.

Figure 25 shows the flow of a storage request. The library server logs the request and moves the request and the object to the resource manager. The resource manager then logs the location of the object and sends the object to the storage subsystem for storing.

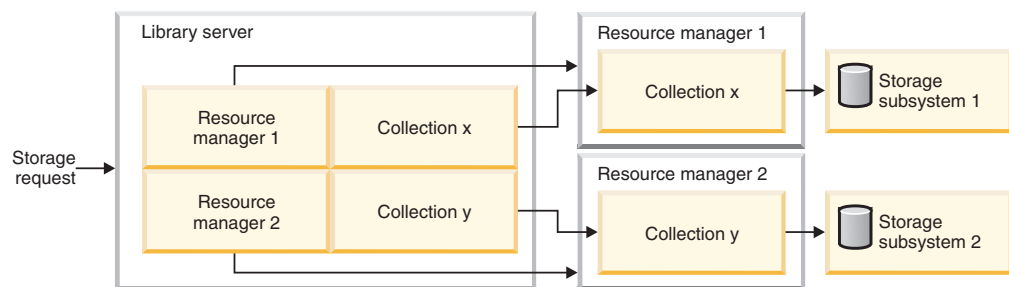


Figure 25. When you store an object, the library server and resource manager log where the object is located..

You migrate objects from high-speed storage devices to low-speed storage devices because storing all objects on high-speed devices is expensive. You need to reserve the high-speed storage devices for those objects that users need to use frequently and, in the case of large media objects, for those objects that need the performance, for example, to play videos or return frequently requested large objects quickly. Large objects and less frequently used objects reside on the slower, yet larger, storage devices.

You must also consider the length of time that you want to keep your content. For example, microfiche can reportedly last 500 years, while content on hard disks degrades much faster.

Replication enhances availability, allowing you to have a replica resource manager available when the main resource manager is not available. You must configure replication ahead of time for this feature to work.

Related concepts

“Resource managers on z/OS” on page 44

Object storage load balancing

By using the system administration client, you can set the default for object storage in the library server configuration for load balancing.

You must assign default resource managers and collections carefully so that the objects are distributed evenly between the resource managers and collections. There are four methods that you can use to ensure that all objects are distributed evenly:

Store objects in the default resource managers and collections from users' profiles

This method works well when you have many users that can create objects.

Store objects in the default resource managers and collections from the item type properties

This method works well when you have many item types.

Store objects in the default resource managers from a user's profile and collections from item type properties (option 1)

Store objects in the default resource managers from item type properties and collections from a user's profile (option 2)

The options in this method are much more flexible and allow greater distribution. This method works well when you have many item types and many users that can create objects.

Important: The two options in this method require the system administrator to define all of the combinations used as valid in the resource managers. Collection names are specific to a resource manager, and mixing them only works if you have each collection defined on all resource managers. Because IBM Content Manager does not check for uniform definitions during define time, invalid combinations can cause store failures that are difficult to troubleshoot. You must ensure that your system is uniform before you implement one of these two options.

File permissions for resource manager object files

File permissions for resource manager object files are determined by values set in the resource manager RMCONFIGURATION database table.

Beginning with Version 8.4.2, the behavior to set file permissions for files stored in the file system by the resource manager is changed. For operating systems such as UNIX that permit these types of settings, the default behavior is to set permissions on a file to read for user with no access for group or others. Two properties in the resource manager RMCONFIGURATION table enable these file permission settings:

- **ICMRM_UMASK**
- **STATIC_FILE_PERMISSION**

The changed file permissions help to strengthen file access protection against accidental changes to sensitive data. Unless a file is being created, updated, or deleted, even the user ID that creates the file will have read-only access to it.

You can change the default file permissions to match behavior in Version 8.3 or Version 8.4 within the limits of the Version 8.4.2 or later permissions. The Version 8.4.2 or later file permission settings do not affect the file permissions on objects that were stored with previous versions of IBM Content Manager.

Important: The effect of the file permission settings depends on the operating system. For example, on a UNIX system and similar operating systems, these settings prevent a read of the file by anyone except the user or a superuser, but the settings do not prevent deletion by the user. On Windows systems, these settings prevent deletion from the command line by all users but result in a confirmation dialog box for deletion in a graphical user interface. The settings do not restrict read by other users. See the documentation for your operating system for more information about how file permission settings affect file management.

ICMRM_UMASK

During the resource manager servlet startup sequence, the **UMASK** process-level system subroutine is called. The **UMASK** system call uses the value from the **ICMRM_UMASK** parameter to set the permissions of files at create time. The default value of the **ICMRM_UMASK** parameter is 077. For a UNIX system or a similar operating system, this value of 077 equals the **UMASK** octal value 077. This value prevents group and others from accessing the files from the time of file creation until the **chmod** command runs when the file is written to storage. For a Windows operating system, the **ICMRM_UMASK** parameter value of 077 equals **S_IREAD | _S_IWRITE**.

For the **ICMRM_UMASK** parameter value, the default value is the most strict value that is allowed. This value creates files with read and write permissions for user and denies read, write, and execute permissions by group and others. You can specify a different value, but that value must not deny read and write permissions by user. The changed value can permit read permission by group or other. If the **ICMRM_UMASK** parameter value is set to a value other than the default, this value is in effect on the file from the time of file creation until the file is written to storage. At that time, the **chmod** command runs to change the file permission to the value set in the **STATIC_FILE_PERMISSION** parameter.

STATIC_FILE_PERMISSION

When a file is written to file system storage, the resource manager runs the **chmod** command to set the default permission for the file when it is not being created, updated, or deleted. The **chmod** system call uses the value from the **STATIC_FILE_PERMISSION** parameter to set the file permissions on the file. The default file permission is 400, a value that permits read by user and denies group and others from accessing the file. Other possible values include 440 (read by user and group), 404 (read by user and others), and 444 (read by user, group, and others). For a Windows system, the **STATIC_FILE_PERMISSION** parameter default value of 400 equals **_S_IREAD**.

Tip: To match the new file permission settings, you might want to consider changing the file permissions of all previously stored data to the default permission for `STATIC_FILE_PERMISSION`, the value 400. However, you must perform this step manually.

Related reference

RMCONFIGURATION

Creating a storage class

Requirement: Before you create a storage class, you must decide which storage type to associate with the storage class.

To create a storage class:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Right-click **Storage Classes** and click **New**. The New Storage Class window opens.
4. In the **Name** field, type 1 to 32 alphanumeric characters as the name of the storage class.
5. Select the proximity of the storage class to the resource manager. The storage class can either be local to the resource manager or remote to it.

Option	Description
Local destination	To identify the storage class as local to the resource manager: <ol style="list-style-type: none">1. Select Local destination. The available device managers are listed.2. From the Assign Device Managers list, select a device manager to assign to the storage class.
Remote destination	To identify the storage class as remote to the resource manager: <ol style="list-style-type: none">1. Select Remote Destination. The resource managers that are available to the current library server are listed.2. From the Resource Manager list, select the remote resource manager that you want the storage class to use.3. In the Collection list, select a collection on the remote resource manager to assign to the objects in this storage class.

6. Click **OK** to save the storage class.

Storage class

Attention: For information pertaining to how to create storage classes, management classes, storage groups, and OAM collections in the z/OS environment, see *IBM z/OS: Object Access Method Planning, Installation, and Storage Administration Guide for Object Support* (SC35-0426).

A *storage class* is a logical grouping of similar storage types that identifies the type of media that an object is stored on. It is not directly associated with a physical location; however, it is directly associated with the device manager, which is the interface between the resource manager and the actual physical location. You can assign only one device manager to each storage class.

Types of storage classes include:

- Fixed disk
- DB2 Content Manager VideoCharger
- Media archive
- Tivoli Storage Manager (including optical, stream, and tape)

When you choose a remote location to create a storage class, you must know the resource manager and collection to which you want objects to move. You cannot assign a device manager to a remote storage class because the device managers are unique to the resource managers in which they are installed. You need to create a valid storage class on the remote resource manager to handle the objects that you want to migrate.

Viewing or modifying a storage class

Restriction: You cannot change a local storage class to a remote storage class or vice versa.

To view or modify a storage class:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Storage Classes** to display all of the storage classes in the right pane.
4. Right-click the storage class that you want to change and click **Properties**. The Properties window opens.
5. Select the proximity of the storage class to the resource manager. The storage class can either be local to the resource manager or remote to it.

Option	Description
Local destination	To identify the storage class as local to the resource manager: <ol style="list-style-type: none">1. Select Local destination. The available device managers are listed.2. From the Assign Device Managers list, select a device manager to assign to the storage class.
Remote destination	To identify the storage class as remote to the resource manager: <ol style="list-style-type: none">1. Select Remote Destination. The resource managers that are available to the current library server are listed.2. From the Resource Manager list, select the remote resource manager that you want the storage class to use.3. In the Collection list, select a collection on the remote resource manager to assign to the objects in this storage class.

6. Click **OK** to save the storage class.

Copying a storage class

To copy a storage class:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Storage Classes** to display all of the storage classes in the right pane.

4. Right-click the storage class that you want to copy and click **Copy**. The Copy Storage Class window opens.
5. In the **Name** field, type 1 to 32 alphanumeric characters as the name of the storage class.
6. Select the proximity of the storage class to the resource manager. The storage class can either be local to the resource manager or remote to it.

Option	Description
Local destination	To identify the storage class as local to the resource manager: <ol style="list-style-type: none"> 1. Select Local destination. The available device managers are listed. 2. From the Assign Device Managers list, select a device manager to assign to the storage class.
Remote destination	To identify the storage class as remote to the resource manager: <ol style="list-style-type: none"> 1. Select Remote Destination. The resource managers that are available to the current library server are listed. 2. From the Resource Manager list, select the remote resource manager that you want the storage class to use. 3. In the Collection list, select a collection on the remote resource manager to assign to the objects in this storage class.

7. Click **OK** to save the storage class.

Deleting a storage class

Requirement: Ensure that there are no objects, management classes, or volumes associated with the storage class.

To delete a storage class:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Storage Classes** to display all of the storage classes in the right pane.
4. Right-click the storage class that you want to delete and click **Delete**.
5. Click **OK** to confirm the deletion.

Creating a device manager

Create a device manager to act as the interface between the resource manager and the storage system.

Prerequisite: The dynamic link library (DLL) or shared library for the device manager must be installed on the workstation where the resource manager is installed before the device manager is created in IBM Content Manager.

To create a device manager:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Right-click **Device Managers** and click **New** to open the New Device Manager window.

4. In the **Name** field, type 1 - 32 alphanumeric characters as the name of the device manager.
5. In the **Description** field, type 1 - 80 alphanumeric characters as a description of the device manager.
6. In the **Parameters** field, type 1 - 254 alphanumeric characters as the parameters for the system to use when it initializes the device manager or when it stores objects on volumes.

Requirement: The following storage system requires the indicated value. Storage systems that are not listed do not have specific requirements.

Storage Type	Operating system	Value
Tivoli Storage Manager with retention protection	any	mode=retention or mode=retention_aggregate

7. In the **Class** field, enter the Java class to be used for this device manager.
8. Select **Enable** or **Disable** to enable or disable the device manager. You might want to disable a device manager when the storage system is unavailable.
9. Click **OK** to save the information and close the window.

Device manager

A *device manager* is software that acts as an intermediary between your resource manager and physical storage. It is the interface between the resource manager and the storage system. You assign device managers to a storage class so that the storage class can communicate with the storage systems defined with it in a migration policy. It communicates the tasks that you define for the resource manager to the storage system where you store your objects.

If the device manager is disabled, the storage systems that use that device manager are inaccessible to the resource manager. You cannot store any new objects on the storage system, and you cannot retrieve any existing objects. You might want to disable a device manager in the following situations:

- When the specific device manager is not installed
- When the specific storage system is not available
- When you want to perform maintenance and you do not want users to access the storage systems that are associated with the device manager

Use the system administration client to create the device managers that you need to access your storage systems. You can assign a device manager to as many storage classes as you want, but a storage class can only have one device manager.

Creating and enabling the ICMZFS device manager

To use the Zettabyte File System (ZFS) as a storage method with the Solaris operating system, you must create a device manager for it. You create and enable the ZFS device manager through the Content Manager EE system administration client.

Before you use ZFS as a storage method, you must set the quota property on each file system in the storage pool and ensure that the total allocations do not exceed the total space available in the storage pool. For example, the following command sets a quota of 50 GB on the `crate/home/jsmith` file system that mounts on `/crate/home/jsmith`.

```
zfs set quota=50G crate/home/jsmith
```

To create and enable the ZFS device manager:

1. In the Content Manager EE system administration client, expand **Resource Managers** and double-click the resource manager (for example, rmdb).
2. Right-click **Device Managers** and select **New**.
3. In the **Name** field, enter ICMZFS.
4. Optional: In the **Description** field, enter a description for this device manager. For example, enter Zettabyte File System.
5. In the **Class** field, enter ZFS.
6. For the **Device manager** choice, select **Enable**. Click **OK** to save the device manager.

Creating and enabling the TSMPOOLED device manager

Use of the TSMPOOLED device manager can help reduce session processor usage for Tivoli Storage Manager connections.

To use the TSMPOOLED device manager, you must configure the Tivoli Storage Manager storage to be nonserial. See the Tivoli Storage Manager documentation for more information about serial and nonserial storage. See also the technical support document about planning for the use of Tivoli Storage Manager with Content Manager EE.


The TSMPOOLED device manager is not defined by default, so you must create and enable it. When you create and enable the device manager, you must complete other tasks required to set up object storage. For example, you must also define a storage class and Tivoli Storage Manager storage volumes for the TSMPOOLED device manager. Also, if the Tivoli Storage Manager server is not defined on the resource manager, you must follow the instructions to add a server definition.

To create and enable the TSMPOOLED device manager:

1. In the Content Manager EE system administration client, expand **Resource Managers** and double-click the resource manager (for example, rmdb).
2. Right-click **Device Managers** and select **New**.
3. In the **Name** field, enter ICMADDMPOOLED.
4. Optional: In the **Description** field, enter a description for this device manager.
5. In the **Class** field, enter TSMPOOLED.
6. For the **Device manager** choice, select **Enable**. Click **OK** to save the device manager.

The TSM_MAX_POOLED_CONNECTIONS, TSM_MAX_WAIT_FOR_FREE_CONNECTION, and TSM_CONNECTION_TIMEOUT parameters in the RMCONFIGURATION table contain default settings for the TSMPOOLED device manager. The default values for these parameters can be changed to match the requirements and available resources of your system.

Related information

 IBM technote: Planning for the use of Tivoli Storage Manager V6.1 and later with DB2 Content Manager V8.4

Device managers by operating system or product

The following table shows the possible device managers and the operating systems on which you can use them. IBM Content Manager installs some of the device managers listed in the table. However, most of the installed device managers are disabled. Other device managers must be installed manually.

Table 66. Device managers and the operating systems or products they work on

Device manager	Operating system or product	Status
ICMADDM	Tivoli Storage Manager	installed and disabled
ICMCIFS	Network-attached storage (NAS) on Windows	installed and disabled
ICMHDDM	Windows	installed and enabled
ICMMADM	Media Archiver	installed and disabled
ICMNFS	Network-attached storage (NAS) on UNIX	installed and disabled
ICMZFS	Zettabyte File System (ZFS) on Solaris	not installed
ICMVCDM	DB2 Content Manager VideoCharger	installed and disabled
ICMFILEPATH	Catalog	installed and enabled
ICMREMOTE	Remote server	installed and enabled
OAM	z/OS	installed and enabled, but only present on z/OS systems

Viewing or modifying a device manager

You might need to modify a device manager when the state of your content management system changes. For example, you might need to disable the device manager when the storage system is unavailable.

To view or modify a device manager:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Device Managers** to display a list of device managers in the right pane.
4. Right-click a device manager and click **Properties**.
5. In the **Description** field, type 1 - 80 alphanumeric characters as a description of the device manager.
6. In the **Parameters** field, type 1 - 254 alphanumeric characters as the parameters for the system to use when it initializes the device manager or when it stores objects on volumes.
7. In the **Class** field, enter the Java class to be used for this device manager.
8. Select **Enable** or **Disable** to enable or disable the device manager.
9. Click **OK** to save the information and close the window.

Copying a device manager

Copying a device manager is a convenient way to set up multiple device managers.

To copy a device manager:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Device Managers** to display a list of device managers in the right pane.
4. Right-click a device manager and click **Copy**.
5. In the **Name** field, type a new name for the device manager.
6. In the **Description** field, type 1 - 80 alphanumeric characters as a description of the device manager.
7. In the **Parameters** field, type 1 - 254 alphanumeric characters as the parameters for the system to use when it initializes the device manager or when it stores objects on volumes.
8. In the **Class** field, enter the Java class to be used for this device manager.
9. Select **Enable** or **Disable** to enable or disable the device manager.
10. Click **OK** to save the device manager and close the window.

Deleting a device manager

To delete a device manager:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Device Managers** to display a list of device managers in the right pane.
4. Right-click a device manager and click **Delete**.
5. Click **OK** to confirm the deletion.

Creating a storage system

Use the system administration client to create the storage systems to store your objects. You must have a storage class already defined when you create your storage system. You must also associate a storage system to a storage group.

“Creating a NAS volume” on page 331

“Creating a local storage volume” on page 333

“Creating a DB2 Content Manager VideoCharger volume” on page 338

“Creating a media archive volume” on page 341

“Creating a Tivoli Storage Manager volume” on page 342

Related concepts

“Resource managers on z/OS” on page 44

Storage system

A *storage system*, which is grouped together with a storage class by a storage group, represents an actual physical device or unit in which the objects in our system are stored. There are different types of storage systems, such as volumes on Windows, file systems on UNIX, DB2 Content Manager VideoCharger, Media Archive, and Tivoli Storage Manager. Storage systems are also known as *volumes*.

When you decide to migrate objects from one storage system to another, you can move them locally or remotely. When you move them locally, the Content Manager EE system provides a list of installed device managers that you can choose to associate with the storage class.

Objects need to exist on certain types of storage systems to retain their integrity. For this reason, Content Manager EE has multiple storage systems where you can store objects:

Table 67. Storage systems supported by IBM Content Manager

	AIX	Linux	Solaris	Windows	z/OS
File system	X	X	X	X	
DB2 Content Manager VideoCharger	X	X		X	
Media archive ¹	X				
Network attached storage (NAS)	X	X	X	X	
Tivoli Storage Manager	X	X	X	X	X
OAM					X

Note: 1. The media archive must be installed on AIX, but it can connect to DB2 Content Manager VideoCharger servers on AIX, Windows, and Linux.

Attention: Storage in the z/OS environment is managed differently than it is in the UNIX and Windows environments.

- For information about how to create storage classes, management classes, storage groups, and OAM collections in the z/OS environment, see *IBM z/OS: Object Access Method Planning, Installation, and Storage Administration Guide for Object Support* (SC35-0426).
- For information about setting up Tivoli Storage Manager in the z/OS environment, see *IBM Tivoli Storage Manager for OS/390 and z/OS Administrator's Guide* (GC32-0775).
- For information about defining OAM and Tivoli Storage Manager collections to the library server, see the discussion of defining resource managers on z/OS.

Different storage system have different setup parameters, but they all use the same four assignments:

Unassigned

Identifies a space on a system, but does not assign it to a storage group. In this case, the resource manager cannot recognize the storage system. This assignment is useful if you want to define several storage systems that you do not have yet or if you do not want to use them at the time that you create them.

Overflow

Identifies a storage system that is available to a storage group but that does not have space enough to hold the objects that it is receiving.

Assigned

Identifies a storage system that belongs to a storage group. You can assign a storage system to one or more storage groups.

Offline

Identifies a storage system that is not mounted or is temporarily unavailable. For example, if you have a disk drive that you can remove from a machine, then you could indicate the disk drive as offline when you detach it so that users cannot store on it. Or, if the LAN connection to a storage system is down, you might have to temporarily take that storage system offline. Content on offline volumes can still be retrieved.

Creating a NAS volume

To create a NAS volume, you complete steps on your network-attached system and then associate the NAS volume with the content management system by using the system administration client.

Resource managers on UNIX and Windows support network-attached storage (NAS) devices. NAS volumes are configured as file system volumes with a few specific settings. For instructions about any step, click **Help** from the window.

1. Create and configure your network-attached storage system. Typically, this task involves the following steps:
 - a. Creating the volumes on the NAS device.
 - b. Setting up the volumes for access.
 - c. Making the NAS volumes available on the resource manager.
 - d. Verifying access across the network.

See *Planning and Installing Your Content Management System* for important considerations about network-attached storage.

2. Connect the NAS volumes, either with a mount command on UNIX or by mapping a network drive on Windows. Verify the connection by viewing a directory listing.
3. Enable the appropriate device manager.

Operating system	Required device manager
UNIX	ICMNFS
Windows	ICMCIFS

To enable a device manager, choose the resource manager you want to work with, click **Device Managers**, and right-click the required device manager. The device manager Properties window opens. In the device manager Properties window, click **Enable**.

Attention: When using the ICMCIFS device manager, the resource manager and its utilities (the migrator, purger, replicator, and stager), which are normally started as services, must be started from the command line.

4. Define a storage class as you would any other storage class, assigning it the device manager you just enabled as a **Local destination**. To define a storage class, choose the resource manager you want to work with, and right-click **Storage Classes**.
5. If you do not intend to use an existing storage group, create a storage group by using the same steps used for any other new storage group. To create a storage group, choose the resource manager you want to work with, and right-click **Storage Groups**.

6. Create a file system volume as you would any other file system volume. To define a file system volume, choose the resource manager you want to work with, then choose **Storage Systems**, and right-click **File System Volumes**. The options for a file system volume slightly depending on whether it is on UNIX or Windows.

Field	Required value
Device (UNIX)	Mounted NAS file system (/dev/lv01, for example)

7. Specify a migration policy. You can use an existing migration policy or create one. Create a migration policy by using the same steps used for any other new migration policy. To create a migration policy, choose the resource manager you want to work with, and right-click **Migration Policies**. You can use an existing migration policy
8. Optional: Define a new collection for use by the NAS volume. To define a collection, choose the resource manager you want to work with, and right-click **Workstation Collections**.

Network-attached storage

Network-attached storage (NAS) is a technology in which an integrated storage system is attached to a messaging network that uses common communication protocols, such as TCP/IP.

A NAS system consists of a controller and a large amount of storage space. The NAS controller focuses on managing disks for storage without attention to the other services and applications that a server normally provides. Because of this structure, NAS typically provides large storage areas with less downtime.

NAS devices can be used in IBM Content Manager as storage systems. There are specific connection requirements for NAS devices, which vary according to the operating system in use on the resource manager. A resource manager on UNIX requires that NAS volumes be mounted with NFS (Network File System). A resource manager on Windows requires that the NAS volumes be mapped using CIFS (Common Internet File System). The NAS device must support the appropriate protocol, either NFS or CIFS, for the resource manager to connect to it.

Make sure that NAS volumes are mounted or mapped, as appropriate, before starting the resource manager.

A critical element of a NAS storage volume is availability. IBM Content Manager does not automatically connect to, or reconnect to, a NAS volume. A NAS volume must be constantly available.

If the network connection is lost, the resource manager will continue to store objects in the connection location. On a Windows system, the connection is to a mapped drive, so it is obvious almost immediately that the connection has been lost. On a UNIX system, however, the mount point is a directory on the local file system. If the connection to the NAS device is lost, the resource manager continues to store objects in the mount directory, and could fill up the file system. For this reason, the mount point for a UNIX NAS device should always be a small file system that is separate from the critical file systems, such as the root file system. This file system should be full enough that no objects can be stored there if the connection to the NAS device is lost.

Always verify the availability of the NAS device to the resource manager before starting the resource manager application. You can verify availability by taking a directory listing or by changing into the mount point directory or mapped drive.

Restriction: Windows does not allow services to see network-attached drives. Therefore, the resource manager and its utilities, which are normally started as services, must be started from the command line.

Creating a local storage volume

You can define a local storage volume by using the system administration client and configuring a file system volume.

“Creating a file system volume on Windows”

“Creating a file system volume on UNIX” on page 335

“Automatic storage system volume suspension” on page 338

Creating a file system volume on Windows

To create a file system volume on Windows:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Right-click **File System Volumes** and click **New** to open the New File System Volume window.
5. In the **Volume label** field, select a name for this volume from the list. The
6. In the **Mount point** field, type a mount point for the volume. A mount point is a logical unit of a device. The device is the physical disk of your machine. For a Windows volume, the mount point is a drive letter.
7. Optional: In the **Default path** field, enter the path on the volume where the resource manager should store the data.
8. In the **Maximum subdirectories** field, type up to 999 as the number of subdirectories created by the resource manager to store objects.

Recommendation: Creating subdirectories to store objects can improve performance.

9. In the **Threshold (begin migration)** field, enter a threshold value. The default for this setting is 100%. When this threshold is reached, the system disables the volume and starts the migrator. The system will enable the volume when normal operation resumes. The volume remains disabled if the target for the migrator is full or stopped. You can also manually enable a volume again.
10. In the **Resume normal operation** field, enter a value. When this limit is reached, the system stops migration, enables the volume again, and creates the buffer for future protection from the threshold.
11. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
12. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.

- Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
13. Click **OK** to save the volume.

Viewing or modifying a file system volume on Windows:

To view or modify a file system volume on Windows:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Click **File System Volumes** to display all the volumes in the right pane.
5. Right-click the volume that you want to view or modify and click **Properties**. The Properties window opens.
6. In the **Mount point** field, type a mount point for the volume. For a Windows volume, the mount point is a drive letter.
7. In the **Volume label** field, type one to 32 alphanumeric characters as the name for this volume.
8. Optional: In the **Default path** field, enter the path on the volume where the resource manager should store the data.
9. In the **Maximum subdirectories** field, type up to 999 as the number of subdirectories created by the resource manager to store objects.

Recommendation: Creating subdirectories to store objects can improve performance.

10. In the **Threshold** field, enter a threshold value. The default for this setting is 100%. If the threshold value is exceeded, the migrator might move objects to keep sufficient disk space available.
11. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
12. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.

- Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.

13. Click **OK** to save the volume.

Copying a file system volume on Windows:

To copy a file system volume on Windows:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Click **File System Volumes** to display the volumes in the right pane.
5. Right-click the volume that you want to copy and click **Copy**.
6. In the **Volume label** field, select a name for this volume from the list.
7. In the **Mount point** field, type a mount point for the volume. For a Windows volume, the mount point is a drive letter.
8. Optional: In the **Default path** field, enter the path on the volume where the resource manager should store the data.
9. In the **Maximum subdirectories** field, type up to 999 as the number of subdirectories created by the resource manager to store objects.

Recommendation: Creating subdirectories to store objects can improve performance.

10. In the **Threshold** field, enter a threshold value. The default for this setting is 100%. If the threshold value is exceeded, the migrator might move objects to keep sufficient disk space available.
11. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
12. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
13. Click **OK** to copy the volume.

Creating a file system volume on UNIX

To create a file system volume on UNIX:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.

4. Right-click **File System Volumes** and click **New** to open the New File System Volume window.
5. In the **Volume label** field, select a device from the list. The device is the physical disk of your machine.
6. In the **Mount point** field, type a mount point for the volume. A mount point is a logical unit of a device.
7. Optional: In the **Default path** field, enter the path on the volume where the resource manager should store the data.
8. In the **Maximum subdirectories** field, type up to 999 as the number of subdirectories created by the resource manager to store objects.

Recommendation: Creating subdirectories to store objects can improve performance.

9. In the **Threshold (begin migration)** field, enter a threshold value. The default for this setting is 100%. When this threshold is reached, the system disables the volume and starts the migrator. The system will enable the volume when normal operation resumes. The volume remains disabled if the target for the migrator is full or stopped. You can also manually enable a volume again.
10. In the **Resume normal operation** field, enter a value. When this limit is reached, the system stops migration, enables the volume again, and creates the buffer for future protection from the threshold.
11. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
12. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
13. Click **OK** to save the volume.

Viewing or modifying a file system volume on UNIX:

To view or modify a file system volume on UNIX:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Click **File System Volumes** to display all the volumes in the right pane.
5. Right-click the volume that you want to view or modify and select **Properties**. The Properties window opens.
6. Optional: In the **Default path** field, enter the path on the volume where the resource manager should store the data.

7. In the **Mount point** field, type a mount point for the volume. A mount point is a logical unit of a device. The device is the physical disk of your machine.
8. In the **Maximum subdirectories** field, type up to 999 as the number of subdirectories created by the resource manager to store objects.

Recommendation: Creating subdirectories to store objects can improve performance.

9. In the **Threshold** field, enter a threshold value. The default for this setting is 100%. If the threshold value is exceeded, the migrator might move objects to keep sufficient disk space available.
10. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
11. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
12. Click **OK** to save the volume.

Copying a file system volume on UNIX:

To copy a file system volume on UNIX:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Click **File System Volumes** to display the volumes in the right contents pane.
5. Right-click the volume that you want to copy and click **Copy**.
6. In the **Device** field, select a device from the list. The device is the physical disk of your machine.
7. Optional: In the **Default path** field, enter the path on the volume where the resource manager should store the data.
8. In the **Mount point** field, type a mount point for the volume. A mount point is a logical unit of a device.
9. In the **Maximum subdirectories** field, type up to 999 as the number of subdirectories created by the resource manager to store objects.

Recommendation: Creating subdirectories to store objects can improve performance.

10. In the **Threshold** field, enter a threshold value. The default for this setting is 100%. If the threshold value is exceeded, the migrator might move objects to keep sufficient disk space available.

11. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
12. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
13. Click **OK** to copy the volume.

Automatic storage system volume suspension

When you create or modify a file system, you can specify options that automatically suspend your storage volume when it is full.

By setting these options, you can prevent errors that might occur when you attempt to write to a full storage system volume.

The resource manager automatically suspends a storage volume in the following conditions:

- When the threshold process detects that a storage volume is over the high threshold setting.

If the storage volume has a migration policy, objects are migrated according to that policy. The threshold process tries to bring the storage volume below the low threshold setting. If the storage volume does not have a migration policy, the storage volume remains suspended until the system administrator acts or until the items waiting to be deleted from the storage volume are cleared.
- When a store or update operation fails because the storage volume is full or when another write IO failure occurs.

Creating a DB2 Content Manager VideoCharger volume

To create a DB2 Content Manager VideoCharger volume:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Right-click **VideoCharger Volumes** and click **New** to open the New VideoCharger Volume window.
5. In the **Asset group** field, type an asset group. This is your preferred name for the volume.
6. In the **Server name** field, select a server name from the list.
7. In the **Threshold** field, enter a threshold value. This is the percentage of total volume that indicates when the DB2 Content Manager VideoCharger Server is

filled to capacity. The default for this setting is 100%. If the threshold value is exceeded, the migrator might move objects to keep sufficient disk space available.

8. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
9. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
10. Click **OK** to save the DB2 Content Manager VideoCharger volume.

Media server

IBM Content Manager can manage multimedia objects like scanned documents, images, text, and presentation files. IBM Content Manager can also manage audio and video files (called *media objects* in IBM Content Manager and *assets* in DB2 Content Manager VideoCharger) by integrating with DB2 Content Manager VideoCharger. IBM Content Manager stores media objects in the DB2 Content Manager VideoCharger Server as assets.

In IBM Content Manager, the DB2 Content Manager VideoCharger Server can bond with the resource manager as a Media Server or Media Resource Manager. To add and configure a DB2 Content Manager VideoCharger Server to IBM Content Manager, see *Planning and Installing DB2 Content Manager VideoCharger*.

Viewing or modifying a DB2 Content Manager VideoCharger volume

To view or modify a DB2 Content Manager VideoCharger volume:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Click **VideoCharger Volumes** to display all the volumes in the right pane.
5. Right-click the volume that you want to view or modify and select **Properties**. The Properties window opens.
6. In the **Asset group** field, type an asset group.
7. In the **Server name** field, select the server name from the list.
8. In the **Threshold** field, enter a threshold value. This is the percentage of total volume that indicates when the DB2 Content Manager VideoCharger Server is filled to capacity. The default for this setting is 100%. If the threshold value is exceeded, the migrator might move objects to keep sufficient disk space available.

9. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
10. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
11. Click **OK** to save the DB2 Content Manager VideoCharger volume.

Copying a DB2 Content Manager VideoCharger volume

To copy a DB2 Content Manager VideoCharger volume:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Click **VideoCharger Volumes** to display the volumes in the right contents pane.
5. Right-click the volume that you want to copy and click **Copy**.
6. In the **Asset group** field, type an asset group. This is your preferred name for the volume.
7. In the **Server name** field, select the server name from the list.
8. In the **Threshold** field, enter a threshold value. This is the percentage of total volume that indicates when the DB2 Content Manager VideoCharger Server is filled to capacity. The default for this setting is 100%. If the threshold value is exceeded, the migrator might move objects to keep sufficient disk space available.
9. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
10. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.

- Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
11. Click **OK** to copy the DB2 Content Manager VideoCharger volume.

Creating a media archive volume

To create a media archive volume:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Right-click **Media Archive Volumes** and click **New** to open the New Media Archive Volume window.
5. In the **Server name** field, select a server name from the list.
6. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
7. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
8. Click **OK** to save the media archive volume.

Viewing or modifying a media archive volume

To view or modify a media archive volume:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Click **Media Archive Volumes** to display all the volumes in the right pane.
5. Right-click the volume that you want to view or modify and select **Properties**. The Properties window opens.
6. In the **Server name** field, select a server name from the list.
7. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
8. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.

- Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
9. Click **OK** to save the media archive volume.

Copying a media archive volume

To copy a media archive volume:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Click **Media Archive Volumes** to display the volumes in the right contents pane.
5. Right-click the volume that you want to copy and click **Copy**.
6. In the **Server name** field, select a server name from the list.
7. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
8. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
9. Click **OK** to copy the media archive volume.

Creating a Tivoli Storage Manager volume

Tivoli Storage Manager is a client/server product that provides storage management and data access services in a heterogeneous environment. It supports various communication methods, provides administrative facilities to manage the backup and storage of files, and provides facilities for scheduling backup operations.

Attention: Tivoli Storage Manager systems in a z/OS environment are configured differently. See the information about resource managers on z/OS for instructions.

To create a Tivoli Storage Manager volume:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Right-click **Tivoli Storage Manager Volumes** and click **New** to open the New Tivoli Storage Volume window.
5. In the **TSM Management class** field, enter the management class. This management class has to be defined on your Tivoli storage system.
6. In the **Server name** field, select a Tivoli server from the list.
7. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
8. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
9. Click **OK** to save the Tivoli Storage Manager volume.

“Modifying the default device manager for use by Tivoli Storage Manager with retention protection” on page 345

Setting up Tivoli Storage Manager with retention protection

IBM Content Manager supports Tivoli Storage Manager with Centera Retention Protection. The definition of the Tivoli Storage Manager storage system is slightly different when retention protection is enabled.

If you have enabled retention protection on your Tivoli Storage Manager system, you must define the Tivoli Storage Manager system by using the specific details provided here. For instructions about any step, click **Help** from the window.

Important: A Tivoli Storage Manager server with retention protection enabled must invoke the proper licensing to transform it into a System Storage® Archive Manager server. Register System Storage Archive Manager, the feature that supports data retention protection, as a licensed feature in Tivoli Storage Manager.

There are two supported retention modes: standard and aggregate. The aggregate retention option improves performance when most of the files being stored are small ones. With aggregate retention, migration does not start until a specified amount of data is ready to be migrated. Configuration is the same for both retention modes, unless otherwise indicated.

Tip: Selecting the correct retention mode can improve migrator performance. You can change between retention modes at any time by changing a few configuration settings.

1. Define the Tivoli Storage Manager system in the resource manager Server Definition Properties window as you would any other Tivoli Storage Manager system. To create a server definition, select the resource manager that you want to work with, and right-click **Server Definitions**.

2. Configure the device manager with a retention mode parameter in the **Parameters** field. To configure a device manager, select the resource manager that you want to work with, and right-click **Device Managers**. Use one of the following parameters:

mode=retention

Use this parameter if you are primarily storing large files.

mode=retention_aggregate

Use this parameter if you are primarily storing small files.

To change from one retention mode to the other, change this parameter.

3. Define a storage class that is used exclusively by the retention-enabled Tivoli Storage Manager server. To define a storage class, select the resource manager that you want to work with, and right-click **Storage Classes**. You will need at a minimum two storage classes. One must not contain retention-controlled volumes. The second must contain retention-controlled volumes.
4. Define the Tivoli Storage Manager volume, but leave it unassigned. To define a Tivoli Storage Manager volume, select the resource manager that you want to work with, then select **Storage Systems**, and right-click **Tivoli Storage Manager Volumes**.
5. Create a new storage group that is used exclusively by the retention-enabled Tivoli Storage Manager system and assign the Tivoli Storage Manager volume to this group. To create a storage group, select the resource manager that you want to work with, and right-click **Storage Groups**.
6. Create a new migration policy that is used exclusively by the retention-enabled Tivoli Storage Manager system and assign the Tivoli Storage Manager storage system to this policy. To create a migration policy, select the resource manager that you want to work with, and right-click **Migration Policies**. The first migration transition must be to a storage class that is not retention controlled. The last transition must be to the class containing the retention volume.
7. Enable or disable aggregation for each source volume in the storage class. To enable aggregation, set the VOL_AGGREGATESIZE value in the RMVOLUMES table to any positive integer. This value indicates, in bytes, how much data should be allowed to aggregate before migration takes place. To calculate the value, multiply the number of megabytes times 1048576, which is the number of bytes in a megabyte:

$size \times 1048576$

For example, to set the value to 5 MB, calculate:

$5 \times 1048576 = 5242880$.

In this case, enter 5242880. If you decide to turn off aggregation, set this value back to 0.

0 Standard retention

positive integer

Aggregate retention

8. Optional: Define a collection that is used exclusively by the retention-enabled Tivoli Storage Manager system. To define a collection, select the resource manager that you want to work with, and right-click **Workstation Collections**.

Modifying the default device manager for use by Tivoli Storage Manager with retention protection

You can update the default device manager, ICMADDMM, for use by Tivoli Storage Manager with retention protection. Complete the following steps:

1. Log on to the system administration client.
2. Update the device manager ICMADDMM:
 - a. Expand Resource Managers in the tree view.
 - b. Expand the resource manager that you want to work with.
 - c. Click **Device Managers** to display a list of device managers in the right pane.
 - d. Right-click ICMADDMM and click **Properties**.
 - e. Update the **Parameters** field with one of the following parameters:

mode=retention

Use this parameter if you are primarily storing large files.

mode=retention_aggregate

Use this parameter if you are primarily storing small files.

To change from one retention mode to the other, change this parameter.

3. Connect to the resource manager database.
connect to *RMDB* user *rmadmin* using *password*
4. View and update the following tables as indicated:

RMCOLLECTIONS

Determine the collection ID and modify the **col_retention** field to support retention. For standard retention, enter 0. For aggregate retention, enter 1.

```
update rmcollections set col_retention=value
```

RMSERVER

Determine from RMSERVER the SVR_SERVERID used for Tivoli Storage Manager.

RMVOLUMES

- a. Determine the VOL_VOLUMEID where VOL_SERVERID matches the SVR_SERVERID you just found.
- b. Update VOL_ATTRIBUTES for this VOL_VOLUMEID and set the value to 100.

Example: From the RMSERVER table, the SVR_SERVERID for Tivoli Storage Manager is 2. From the RMVOLUMES table, the VOL_VOLUMEID matching VOL_SERVERID=2 is 3. The update to the resource manager database is then:

```
update rmvolumes set vol_attributes=100  
where vol_volume=3
```

5. Restart the resource manager.

Viewing or modifying a Tivoli Storage Manager volume

To view or modify a Tivoli Storage Manager volume:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.

4. Click **Tivoli Storage Manager Volumes** to display all the volumes in the right pane.
5. Right-click the volume that you want to view or modify and select **Properties**. The Properties window opens.
6. In the **TSM Management class** field, enter a management class. This management class has to be defined on your Tivoli storage system.
7. In the **Server name** field, select the server name from the list. This is the name for the Tivoli server.
8. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
9. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.
 - Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
10. Click **OK** to save the Tivoli Storage Manager volume.

Copying a Tivoli Storage Manager volume

To copy a Tivoli Storage Manager volume:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Expand **Storage Systems**.
4. Click **Tivoli Storage Manager Volumes** to display the volumes in the right contents pane.
5. Right-click the volume that you want to copy and click **Copy**.
6. In the **TSM Management class** field, enter the management class. This management class has to be defined on your Tivoli storage system.
7. In the **Server name** field, select a server name from the list. This is the name for the Tivoli server.
8. In the **Storage class** field, select a storage class to associate with this volume from the list. You can associate only one storage class with each volume. A storage class identifies the type of media that an object is stored on.
9. In the **Assignment** field, click a radio button to assign a relationship between the IBM Content Manager volume and one or more storage groups.
 - Select **Unassigned** to prevent storage groups from using this volume as storage.
 - Select **Overflow** to use the volume as overflow for all storage groups. Overflow volumes store objects when all other volumes for a storage group are full.

- Select **Assigned** to associate the volume to the storage groups that you select in the **Assign one or more storage groups** list. Selecting **Assigned** enables the **Suspend Storage** check box. Select **Suspend storage** to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.
 - Select **Offline** to prevent storing to the volume. **Optional:** In the **Offline location** field, indicate the location of the volume.
10. Click **OK** to copy the Tivoli Storage Manager volume.

Deleting a storage system

To delete a storage system:

Restriction: A file system volume that is assigned to a group cannot be deleted. To delete the file system volume, you must first remove it from the group.

1. Migrate all of the objects from the storage system.
2. Expand **Resource Managers** in the tree view.
3. Expand the resource manager that you want to work with.
4. Expand **Storage Systems**.
5. Double-click the folder of the type of storage system that you want to delete to display all of those storage systems in the right pane.
6. Check the storage group to make sure that the class status for that storage system is set to Unassigned.
7. Right-click the storage system that you want to delete and click **Delete**.
8. Click **OK** to confirm the deletion.

Replacing or repartitioning a hard disk

If a volume or file system that is used by your resource manager becomes full, you can replace or repartition the physical disk on which it is located to make more space available.

Replacing or repartitioning the disk makes the information stored in the volumes table (RMVOLUMES) for that volume or file system invalid.

Replacing the staging volume on UNIX

The directory for the staging volume is in the resource manager database table, RMSTAGING. Follow these steps to replace the staging volume. Replace the following variables in your SQL statements with values that are correct for your system:

rmadmin

Resource manager administrator ID

password

Password for the resource manager administrator ID

staging_path

Location of the staging directory, as an absolute path with the trailing slash

1. Change the permissions on the new staging directory to match those of your resource manager ID or what is currently in place for the existing staging directory

2. Update the location of your staging volume in the resource manager database. Open a DB2 command prompt and enter the following commands, each on a new line:

```
connect to rmdb user rmdadmin using password
update rmstaging set sta_path=staging_path
```

Replacing the staging volume on Windows

The directory for the staging volume is in the resource manager database table, RMSTAGING. Follow these steps to replace the staging volume. Replace the following variables in your SQL statements with values that are correct for your system:

rmdadmin

Resource manager administrator ID

password

Password for the resource manager administrator ID

staging_path

Location of the staging directory, as an absolute path including the drive letter

1. Change the permissions on the new staging directory to match those of your resource manager ID or what is currently in place for the existing staging directory
2. Update the location of your staging volume in the resource manager database. Open a DB2 command prompt and enter the following commands, each on a new line:

```
connect to rmdb user rmdadmin using password
update rmstaging set sta_path=staging_path'
```

3. Update the location of your staging volume in the resource manager database. Enter the following commands at a DB2 command prompt:

```
connect to rmdb user rmdadmin using password
update rmstaging set sta_path=staging_path
```

Replacing the storage volume on UNIX

The resource manager uses the following scheme to develop the path.

vol_path + the *string_table* value of *lbosdata* + *collection* + *num_bucket_value*

The *logical_volume* and *mount_point* are used in various calls to get file system information.

Follow these steps to update the resource manager storage volume. Replace the following variables in your SQL statements with values that are correct for your system:

rmdadmin

Resource manager administrator ID

password

Password for the resource manager administrator ID

staging_path

Location of the staging directory, as an absolute path with the trailing slash

ID

Volume ID

1. Change the permissions on the new staging directory to match those of your resource manager ID or what is currently in place for the existing staging directory.
2. Copy all of the existing files to the new storage volume:

```
cp -rp current_staging_directory new_staging_directory
```
3. Open a DB2 command prompt.
4. Update the location of your storage volume in the resource manager database. Use `df -k` to determine the FILESYSTEM and MOUNTED ON location for the new staging directory. To update the storage volume, enter the following commands, each on a new line:

```
connect to rmdb user rmadmin using password
select vol_volumeid,vol_logicalname,vol_mountpoint from rmvolumes
```
5. Determine which VOLUMEID is the one that you need to change and change it. Enter the following commands, each on a new line:

```
update rmvolumes set vol_logicalname=staging_path where
vol_volumeid=ID
update rmvolumes set vol_mountpoint=staging_path where
vol_volumeid=ID
update rmvolumes set vol_size=0 where vol_volumeid=ID
update rmvolumes set vol_path=staging_path where
vol_volumeid=ID
update rmvolumes set vol_freespace=0 where vol_volumeid=ID
```

Notice that the last two steps force the resource manager to recalculate the volume space and capacity during any new store operations. These values are reflected in the RMVOLUMES tables when the resource manager shuts down.

Replacing the storage volume on Windows

If you replace or repartition the hard disk that contains the LBOSDATA directory, you need to identify the new configuration to your system. Replace the following variables in your SQL statements with values that are correct for your system:

ID Volume ID

label Partition label

X Drive letter

1. Restore the LBOSDATA directory to the new disk or partition.
2. Open a DB2 command prompt.
3. Edit the volumes table to change the following columns to zero for the volume that has been changed. Enter each command on a new line:

```
update rmvolumes set vol_size=0 where vol_volumeid=ID
update rmvolumes set vol_freespace=0 where vol_volumeid=ID
```

The next time the resource manager writes or deletes an object, the information is read from the new disk or partition and placed in the volumes table.

4. If your volume is on a different partition, then manually edit the RMVOLUMES table to update the VOL_LOGICALNAME and VOL_MOUNTPOINT values. Enter the following commands, each on a new line:

```
update rmvolumes set vol_logicalname=label where vol_volumeid=ID
update rmvolumes set vol_mountpoint=X: where vol_volumeid=ID
```
5. Start the resource manager.

Creating a storage group

Attention: For information about how to create storage classes, management classes, storage groups, and OAM collections in the z/OS environment, see IBM *z/OS: Object Access Method Planning, Installation, and Storage Administration Guide for Object Support* (SC35-0426).

Requirement: You must create the storage systems that you want to associate with the storage group before you create the storage group.

You can associate multiple storage systems with a storage group.

To create a storage group:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Right-click **Storage Groups** and click **New**. The New Storage Group window opens.
4. In the **Name** field, type 1 to 32 alphanumeric characters as the name for this storage group.
5. The **Storage systems** list identifies the available storage systems. Select the storage systems that you want to associate with this storage group.

Recommendation: When you create your IBM Content Manager system, assign a different storage system for each storage group and a different storage group for each collection.

6. Click **OK** to save the storage group.

Related concepts

“Resource manager” on page 41

Storage group

A *storage group* contains one or more storage systems and storage classes. It associates each storage system to a storage class.

Storage groups contain the identities of the storage systems and storage classes that you use to store the objects in a collection. A storage group is one of two essential components that creates a collection. The other component that creates a collection is the migration policy. The migration policy is the path that objects take when they move from one storage class to another. For example, you could have storage groups for high demand data and storage groups in low demand data (disk versus tape).

The migration policy contains a list of storage classes. Through the storage class to storage system association, the objects know the storage system to which they belong, and through the migration policy, they know the storage system to which they will move next.

You must create the necessary storage systems and storage classes before you can create a storage group.

Recommendation: When you create your IBM Content Manager system, assign a different storage system for each storage group and a different storage group for each collection.

Viewing or modifying a storage group

To view or modify a storage group:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Storage Groups** to display all of the storage groups in the right pane.
4. Right-click the storage group that you want to change and click **Properties**. The Properties window opens.
5. The **Storage systems** list identifies the available storage systems. Select the storage systems that you want to associate with this storage group.

Recommendation: When you create your IBM Content Manager system, assign a different storage system for each storage group and a different storage group for each collection.

6. Click **OK** to save the storage group.

Copying a storage group

To copy a storage group:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Storage Groups** to display all of the storage groups in the right pane.
4. Right-click the storage group that you want to copy and click **Copy**. The Copy window opens.
5. In the **Name** field, type 1 to 32 alphanumeric characters as the name for this storage group.
6. The **Storage systems** list identifies the available storage systems. Select the storage systems that you want to associate with this storage group.

Recommendation: When you create your IBM Content Manager system, assign a different storage system for each storage group and a different storage group for each collection.

7. Click **OK** to save the storage group.

Deleting a storage group

Requirement: Ensure that there are no storage systems that are associated with the storage group and no collections or volumes that reference the storage group.

To delete a storage group:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Storage Groups** to display all of the storage groups in the right pane.
4. Right-click the storage group that you want to delete and click **Delete**.
5. Click **OK** to confirm the deletion.

Creating a migration policy

Prerequisite: You must create the necessary storage classes for a migration policy before you can create the migration policy.

To create a migration policy:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Right-click **Migration Policies** and click **New**. The New Migration Policy window opens.
4. In the **Name** field, type one to 32 alphanumeric characters as the name for the migration policy.
5. Click **Add** to open the New Migration Policy Entry window where you can define a new storage class and a retention period. A retention period is how long the objects remain in that storage class. That information is then added to the local step list in the New Migration Policy window.
6. To modify the properties of a migration step, select a step from the list and click **Edit** to open the Edit Migration Policy window.
7. If you want to migrate the collection to a remote storage system, you must select **Move to remote storage class** and select a storage class from the list to move the object to another resource manager. Only remote storage classes are in the list. Each storage class is associated with one or more storage systems. The remote storage class must exist. The storage class you designate as the remote storage class identifies a resource manager and collection with which it belongs. If you add a remote storage class to the migration policy, it is the last step in the migration policy. If **Move to remote storage class** is not selected, the last step must have a retention period of **forever**.
8. Click **OK** to save the migration policy.

After you create your migration policy, you must assign it to a collection. If you do not assign it to a collection, then it does not get used, even when you only have one collection defined in your resource manager.

Migration policy

Attention: For information about how to create storage classes, management classes, storage groups, and OAM collections in the z/OS environment, see IBM *z/OS: Object Access Method Planning, Installation, and Storage Administration Guide for Object Support* (SC35-0426).

A *migration policy* is a user-defined schedule for moving objects from one storage class to the next. It describes the retention and class transition characteristics for a group of objects in a storage hierarchy. Creating a migration policy and defining the migrator schedule automates the migration of objects so you do not have to manually monitor migration.

Each migration policy belongs to a collection of objects and contains the rules for migrating the objects in that collection. When you create your migration policy, you decide how long to store a collection in a storage system. You use a migrator schedule to check the migration policy for collections for which time has expired.

When the migrator schedule begins, and the time for the collection in its current storage class has elapsed, then the migration policy moves the collection to the

next storage class. The storage class determines the location, which is limited to the storage systems in the storage group that is assigned to the collection to which the object belongs. You must create the storage classes before you can create the migration policy. To migrate an object to another resource manager, specify a remote storage class as the final step in a migration policy.

Attention: Tivoli Storage Manager calls its migration policies management classes.

You specify when you want the migrator to run on the Migrator Schedule page of the Resource Manager Configuration window. There is also a **Migrator** field on the Cycles page where you specify when the migrator wakes up to check the schedule and determine what needs to migrate.

An object is set to migrate according to the retention period specified in its migration policy. However, if the volume becomes full, the object might migrate early because of threshold migration. The threshold cycle is the amount of time in hours and minutes that must elapse before the system checks the capacity of volumes. You specify the threshold cycle in the **Threshold** field on the Cycles page of the Resource Manager Configuration window. Threshold migration works just like normal migration, except that it occurs when the volume space exceeds the threshold.

You can use the same migration policy for more than one collection.

Viewing or modifying a migration policy

To view or modify a migration policy:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Migration Policies** to display all the migration policies in the right pane.
4. Right-click the migration policy that you want to change and click **Properties**. The Properties window opens.
5. Click **Add** to open the New Migration Policy Entry window where you can define a new storage class and a retention period. A retention period is how long the object remains in that storage class. That information is then added to the local step list in the New Migration Policy window. To modify the properties of a migration step, select a step from the list and click **Edit** to open the Edit Migration Policy window.
6. Select **Move to remote storage class** and select a storage class from the list to use a storage class that places the object on another resource manager. Only remote storage classes are in the list. If you add a remote storage class to the migration policy, it is the last step in the migration policy.
7. Click **OK** to save the migration policy.

Objects that are already committed to an existing migration policy do not move when you change the migration policy. However, they follow the new migration policy when the time expires for the storage system they are on. You can manually change the action date by connecting to your resource manager and updating the OBJ_ACTIONDATE field.

Copying a migration policy

To copy a migration policy:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Migration Policies** to display all the migration policies in the right pane.
4. Right-click the migration policy that you want to copy and click **Copy**. The Copy window opens.
5. In the **Name** field, type one to 32 alphanumeric characters as the name for the migration policy.
6. Click **Add** to open the New Migration Policy Entry window where you can define a new storage class and a retention period. A retention period is how long the object remains in that storage class. That information is then added to the local step list in the New Migration Policy window. To modify the properties of a migration step, select a step from the list and click **Edit** to open the Edit Migration Policy window.
7. Select **Move to remote storage class** and select a storage class from the list to use a storage class that places the object on another resource manager. Only remote storage classes are in the list. If you add a remote storage class to the migration policy, it is the last step in the migration policy.
8. Click **OK** to save the migration policy.

Deleting a migration policy

Important: Ensure that there are no collections that are associated with the migration policy.

To delete a migration policy:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Migration Policies** to display all the migration policies in the right pane.
4. Right-click the migration policy that you want to delete and click **Delete**.
5. Click **OK** to confirm the deletion.

Creating a migration policy entry

To create a migration policy entry:

1. Open the New Migration Policy window.
2. Click **Add** to open the Add Migration Policy Entry window.
3. In the **Storage class** field, select a storage class from the list.
4. Specify a retention period. A retention period is how long the object remains in that storage class.
5. Click **OK** to save the migration policy entry.

Viewing or modifying a migration policy entry

To view or modify a migration policy entry:

1. Open the New Migration Policy window.
2. Click **Edit** to open the Edit Migration Policy Entry window.
3. In the **Storage class** field, select a storage class from the list.

4. Specify a retention period. A retention period is how long the object remains in that storage class.
5. Click **OK** to save the migration policy entry.

Changing the date of migration

You can specify when you want the system to migrate objects from one type of storage to another.

When you migrate objects, you need to configure settings for how long you want to retain a collection, and when to check for migrating the collections.

1. The first task is to decide how long you want to retain a collection. You designate the retention period when you create a migration policy. You have two choices, either you keep the collection in a storage system for a certain number of days, or, you keep the collection in a storage system forever. You can change the amount of time by viewing the properties of a migration policy, selecting the storage class that you want to change, and clicking **Edit**. In the window that opens, you can change the amount of time of the storage class to its new time.
2. The second task is to configure the migrator schedule for your resource manager. You can find the migrator schedule by completing the following steps:
 - a. Expand **Resource Managers** in the tree view.
 - b. Expand the resource manager that contains the migration policy in which you want to schedule.
 - c. Right click **Configurations**.
 - d. Click the **Migrator Schedule** tab.
3. You must decide when you want the migration of objects to occur. You have two choices in the panel: **Every day** or **Specific day**. The time you select starts the migrator schedule to check if the retention period of the collection in a migration policy has expired. If the time has expired, then the resource manager moves the collection to the next storage class listed in the migration policy.

Migrating and purging the DB2 Content Manager VideoCharger Server media objects at regular intervals

To configure how often to migrate and purge media objects to the Multimedia Archive at regular intervals, complete the following steps:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that manages the DB2 Content Manager VideoCharger server that contains the schedule for migrating and purging.
3. Right-click **Configurations**, then right-click the name of the configuration that the DB2 Content Manager VideoCharger server uses. The Resource Manager Configuration window opens.
4. Click the **Cycles** tab.
5. On the Cycles tab, provide values for the **Purger** and **Migrator**.
6. Set how often to purge and migrate by typing the corresponding **Hours** and **Minutes**.
7. Under Batches (files), set how many files you want to migrate simultaneously by typing a number for **Stager** and **Migrator**. The default is 50 files.
8. Click **OK** to save your changes and close the window.

IBM Content Manager then automatically starts, enables, and stops both the stager and the migrator during the intervals you specified.

Creating a collection

Attention: For information about how to create storage classes, management classes, storage groups, and OAM collections in the z/OS environment, see IBM *z/OS: Object Access Method Planning, Installation, and Storage Administration Guide for Object Support* (SC35-0426).

Restriction: To define a collection, you must have one of these system-defined privileges:

- ICM_PRIV_DOMAIN_ADMIN
- ICM_PRIV_SUPER_DOMAIN_ADMIN
- ICM_PRIV_DOMAIN_DEFINE_SMS_COLL

Prerequisite: You must create the storage group and migration policy that you want to use in the collection before you create the collection.

To create a collection:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Right-click **Workstation Collections** and click **New** to open the New Workstation Collection window.
4. In the **Name** field, type 1 to 44 characters as a name for the collection. Collection names for text-searchable documents must not contain spaces. Collection names for use with DB2 Universal Database must not rely on case for uniqueness, because the DB2 database is not case sensitive. The best practice is to assign names that are unique without regard to case, even if the database is case sensitive.
5. From the **Migration policy** list, select a default migration policy for the collection.
6. From the **Storage group** field, select a default storage group for the collection.
7. If you have enabled administrative domains, select a domain from the list in the **Domain** field. Because the collection is a part of the resource manager, the domain that you select must be the same as the domain that you selected when you defined the resource manager. See the related information about creating administrative domains for detailed instructions and restrictions.
8. You can replicate objects in this collection to several other collections that are on different resource managers.
 - a. Click **Add** to open the New Workstation Collection Entry window.
 - b. In the **Resource manager** field, select the target resource manager. This target is the resource manager to which you want to replicate objects.
 - c. In the **Collection** field, select the target collection. This target collection is on in the target resource manager.
 - d. Click **OK** to return to the New Workstation Collection window.
9. Optional: You can set priorities for the targets that you have defined. For example, if you defined three target resource managers, you can select one of these three targets and click **Move up** to move it to the top of the list. Then,

when you are retrieving replicated objects, you retrieve them from that resource manager first. You retrieve based on the order that the resource managers display in the table.

10. Click **OK** to save the information and close the window.

Related tasks

“Creating administrative domains” on page 517

Selecting a target resource manager and collection

As part of your replication options, you define target resource managers and collections to which you want to replicate objects. To define a target resource manager and collection:

1. Open the New Workstation Collection window.
2. Select the **Enable collection for replication** check box and click **Add** to open the New Workstation Collection Entry window.
3. In the **Resource manager** field, select the target resource manager. This target is the resource manager to which you want to replicate objects.
4. In the **Collection** field, select the target collection. This target collection is in the target resource manager.
5. Click **OK** to return to the New Workstation Collection window. In this window.
6. Optional: In the New Workstation Collection window, you can set priorities for the targets that you defined. For example, if you defined three target resource managers, you can select one of these three targets and click **Move up** to move it to the top of the list. Then, when you are retrieving replicated objects, you retrieve them from that resource manager first.

Defining OAM collections

Before you can define OAM collections to the library server, you must define your collections in OAM.

When you associate those collections with IBM Content Manager user IDs and item types, the storage class and management class policies of the collection dictate the placement of IBM Content Manager objects to a certain storage group. The policies also dictate the timing of the migration and backup for the objects. However, the collections defined to OAM must also be made known to the IBM Content Manager library server.

You select a default collection and prefetch collection during the library server installation. To inform the library server of additional OAM collections for a z/OS resource manager:

1. Expand **Resource Managers** in the tree view.
2. Expand your resource manager.
3. Right-click **MVS Collections** and click **New** to open the MVS™ Collection window.
4. Enter the name of the OAM collection that you want to add.
5. The MVS Collection window includes a **Prefetch collection** check box. Check this box if this collection is to be used as a prefetch collection. A prefetch collection is one that stores objects that are retrieved often and purged frequently. Typically, prefetch collections store objects on fast disk storage.
6. You can specify target managers and collections for replication. Use the **Add** and **Delete** buttons to add or remove resource managers and collections and

the **Move up** and **Move down** buttons to change the order of the resource managers and collections. The order of the resource managers and collections is important because the order indicates which replica should be attempted first, second, third, and so on, if the primary (or other replica) is unavailable.

Defining Tivoli Storage Manager collections on z/OS

You can define Tivoli Storage Manager collections on a z/OS resource manager.

Attention: You must first set up the Tivoli Storage Manager collection using the Tivoli Storage Manager administration client. See IBM Tivoli Storage Manager for OS/390 and z/OS *Administrator's Guide* (GC32-0775).

When you associate those collections with IBM Content Manager user IDs and item types, the collection's storage class and management class policies dictate the placement of IBM Content Manager objects to a certain storage group, as well as the timing of the objects' migration and backup. However, the collections must also be made known to the IBM Content Manager library server.

You select a default collection and prefetch collection during the library server installation.

To define Tivoli Storage Manager collections for a z/OS resource manager:

1. Log into the resource manager database and open a DB2 command prompt.
2. Insert a row for each Tivoli Storage Manager server in the ICMRMSEVER table. If you have already defined the servers, and want to add another collection, you do not need to insert a new row into this table.

```
INSERT INTO ICMRMSEVER VALUES
(server_ID, 'server_type', 'server_name',
'server_protocol', 'server_user_ID', 'server_password',
'server_hostname', server_port, 'server_schema',
'server_path', 'server_platform', 'opt_location',
mount_wait, buffer_size, compression,
mode, 'node_name', 'application_type',
'opt_file', 'file_space_type')
```

where

server_ID

Server ID. This is a unique numeric identifier for this record. Increment this value by 1 from the last row in the table.

server_type

Type of server. This is an alphanumeric value.

server_name

Server name. Use the Tivoli Storage Manager node name.

server_protocol

Protocol used to access the server.

server_user_ID

Server connection user ID.

server_password

Password for *server_user_ID*.

server_hostname

Fully qualified server host name.

server_port
Port used by the server.

server_schema
Server database schema.

server_path
Server path.

server_platform
Operating system used by the server.

opt_location
Location of the Tivoli Storage Manager options file. Do not include the file name.

mount_wait
Flag for wait/not wait for drive mounts. Use 0 to not wait or 1 to wait.

buffer_size
Tivoli Storage Manager buffer size used during write operations, in kilobytes.

compression
Enable or disable compression. Use 0 to disable compression or 1 to enable it.

mode Backup or archive mode. Use 0 for backup or 1 for archive.

node_name
Tivoli Storage Manager node name.

application_type
Optional label on the file space. Suggested values: leave blank or use a meaningful string to identify the client application as the IBM Content Manager resource manager.

opt_file Fully qualified name of the Tivoli Storage Manager options file.

file_space_type
File space type. View the properties of the file space name using the Tivoli Storage Manager Server Administration tool.

For example:

```
INSERT INTO ICMRMSERVER VALUES
(0,'TSM','IMWEBSR1',
 'HTTP','dwayne','password',
 'ctfmvs97.raleigh.ibm.com',1580,'IFVTA',
 '/usr/lpp/Tivoli/tsm/client/api/bin','UNIX',
 '/usr/lpp/Tivoli/tsm/client/api/bin/dsm.opt',
 0,0,0,
 0,'TSMRM','',
 '', 'CM_FILESPACE')
)
```

3. Add the following row for each Tivoli Storage Manager collection in the ICMRMMGMTCLASS table in the resource manager database. If you have already defined your management classes, you do not need to update this table again.

```
INSERT INTO ICMRMMGMTCLASS VALUES
(management_class_ID, 'collection_management_class')
```

where

management_class_ID

Unique identifier for this row in the table. Increment this value by 1 from the last row in the table.

collection_management_class

The type of media. Typical entries are DISK, OPTICAL, TAPE, and DEFAULT.

4. Add the following row for each Tivoli Storage Manager collection in the ICMRMCOLLECTION table in the resource manager database:

```
INSERT INTO ICMRMCOLLECTION VALUES
(collection_code, 'collection_name',
'collection_management_class', collection_server_ID);
```

where

collection_code

Unique identifier for this row in the table. Increment this by 1 from the last row in the table.

collection_name

The name you defined in the system administration client for the MVS collection.

collection_management_class

The collection management class, as defined in the ICMRMMGMTCLASS table.

collection_server_ID

The ID of the collection server. This value must match the server ID the ICMRMSERVER table.

5. Define the Tivoli Storage Manager collection to the library server as you would define an OAM collection.

Collection

A *collection* is a group of related objects that are stored in the same storage group and are managed by the same migration policy. It is the last component that you define for object storage because it requires a storage group and migration policy.

A collection identifies a group of related objects with similar storage management criteria. All objects in a collection are stored on the storage systems specified in the storage group of that collection. All objects in the collection migrate according to the rules that are defined for the migration policy in that collection.

There are two predefined collections that you can use, or you can create your own collections. The predefined collections are TABLE.CLLCT001 and CBR.CLLCT001. TBL.CLLCT001 is a BLOB (binary large object) collection. CBR.CLLCT001 is a file system collection.

Tip: Use the BLOB collection for collections of small objects. If you have large objects, for example ones that are primarily larger than 20 KB each, the file system collection will provide faster performance.

A storage group contains the identities of the storage systems and storage classes that you use to store the objects in a collection. A storage group is one of two essential components that creates a collection. The other component that creates a

collection is the migration policy. The migration policy is the path that objects take when they move from one storage class to another.

Recommendation: When you create your content management system, assign a different storage system for each storage group and a different storage group for each collection.

Related concepts

“Resource manager” on page 41

Viewing or modifying a collection

To view or modify a collection:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Workstation Collections** to display all the collections in the right pane.
4. Right-click the workstation collection that you want to change and click **Properties**. The Properties window opens.
5. From the **Migration policy** list, select a default migration policy for the collection.
6. From the **Storage group** field, select a default storage group for the collection.
7. If you have enabled administrative domains, select a domain from the list in the **Domain** field. Because the collection is a part of the resource manager, the domain that you select must be the same as the domain that you selected when you defined the resource manager.
8. You can replicate objects in this collection to several other collections that are on different resource managers.
 - a. Click **Add** to open the New Workstation Collection Entry window.
 - b. In the **Resource manager** field, select the target resource manager. This target is the resource manager to which you want to replicate objects.
 - c. In the **Collection** field, select the target collection. This target collection is on in the target resource manager.
 - d. Click **OK** to return to the New Workstation Collection window.
9. Optional: You can set priorities for the targets that you have defined. For example, if you defined three target resource managers, you can select one of these three targets and click **Move up** to move it to the top of the list. Then, when you are retrieving replicated objects, you retrieve them from that resource manager first. You retrieve based on the order that the resource managers display in the table.
10. Click **OK** to save the collection.

Copying a collection

To copy a collection:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Click **Workstation Collections** to display all the collections in the right pane.
4. Right-click the workstation collection that want to copy and click **Copy** to open the Copy window.
5. In the **Name** field, type 1 to 44 characters as a name for the collection. Collection names for text-searchable documents must not contain spaces.

Collection names for use with DB2 Universal Database must not rely on case for uniqueness, because the DB2 database is not case sensitive. The best practice is to assign names that are unique without regard to case, even if the database is case sensitive.

6. From the **Migration policy** list, select a default migration policy for the collection.
7. From the **Storage group** field, select a default storage group for the collection.
8. If you have enabled administrative domains, select a domain from the list in the **Domain** field. Because the collection is a part of the resource manager, the domain that you select must be the same as the domain that you selected when you defined the resource manager.
9. You can replicate objects in this collection to several other collections that are on different resource managers.
 - a. Click **Add** to open the New Workstation Collection Entry window.
 - b. In the **Resource manager** field, select the target resource manager. This target is the resource manager to which you want to replicate objects.
 - c. In the **Collection** field, select the target collection. This target collection is on in the target resource manager.
 - d. Click **OK** to return to the New Workstation Collection window.
10. Optional: You can set priorities for the targets that you have defined. For example, if you defined three target resource managers, you can select one of these three targets and click **Move up** to move it to the top of the list. Then, when you are retrieving replicated objects, you retrieve them from that resource manager first. You retrieve based on the order that the resource managers display in the table.
11. Click **OK** to save the collection.

Deleting a collection

Important: Ensure that there are no objects that are associated with the collection and no user IDs or item types that reference the collection. Use the client for Windows or another client application to query the library server for items, users, and so forth. Also allow the migrator to run before actually deleting the collection.

To delete a collection:

1. Expand **Resource Managers** in the tree view.
2. Expand the resource manager that you want to work with.
3. Double-click **Workstation Collections** to display all of the collections in the right pane.
4. Right-click the workstation collection that you want to delete and click **Delete**.
5. Click **OK** to confirm the deletion.

Setting up replication

To set up replication, you must define your resource managers to the library server, define each resource manager to each other, and define your collections.

When you define a replica resource manager to a library server, you define a connection between a primary resource manager collection and a replica resource manager collection. A replication process initiated by the administrator replicates stored objects from the primary resource manager collection to the replica resource

manager collection. In the following steps, an example is used to help clarify the steps that you must complete. In the example, the primary resource manager is *RMDB1* and the replica resource manager is *RMDB1_replica1*.

To set up replication:

1. From the system administration client, expand the library server in the tree view, right-click **Resource Manager**, and click **New** to define the *RMDB1* resource manager.

Requirement: Each of the primary and replica resource managers must point to the same library server.

- a. Supply information for the fields to define a resource manager to the library server, for example, *RMDB1* for the **Name** field.
 - b. Select the operating system for the resource manager application in the **Application server operating system** field. The default collection for the resource manager is generated based on the selection that you make in the **Application server operating system** field.
 - c. Click **OK** to save the new resource manager definition.
2. Optional: Create a new collection in the resource manager to be replicated. In the system administration client tree view, add collections for the *RMDB1* resource manager. (You can also use one of the default collections as the collection to be replicated.)
 - a. Expand the *RMDB1* resource manager to display the collection type. If the operating system of the resource manager application is z/OS, the collection type is **MVS Collections**. For any other operating system, the collection type is **Workstation Collections**.
 - b. Right-click the collection type to create a collection for the resource manager. Type a name, select a migration policy, and enter other required data for the new collection. For a collection on a z/OS resource manager, only the name of the collection is required.
3. Repeat the process used in Step 1 to define the *RMDB1_replica1* resource manager to the library server. If you do not want to use one of the default collections for *RMDB1_replica1* as the replica collection, use the process in Step 2 to define collections for *RMDB1_replica1*.
4. Add the information for the replica resource manager *RMDB1_replica1* to *RMDB1*.
 - a. Expand the *RMDB1* resource manager and select the collection type to display the collections.
 - b. Right-click the collection name for which you want to create a replica and click **Properties**.
 - c. In the Collection Properties window, click **Add** to enable the collection for replication and to add the replica information.
 - d. In the New Workstation Collection window, select *RMDB1_replica1* as the replica resource manager and select a collection name for the replica.
 - e. Save your selections on the New Workstation Collection window and Collection Properties window to complete the setup for replication.

In this example, the collection selected for *RMDB1* is the source collection that replicates to the target collection on *RMDB1_replica1*.

Related reference

“Troubleshooting replication” on page 647

Replication

Replication provides added security, helping to ensure that an object is available for retrieval or update if the resource manager that contains the primary object is offline.

Replication is a feature of IBM Content Manager with which you can create one or more replicas for an object when it is first created. To enhance retrievability and security, you can replicate object data from a primary resource manager to a replica resource manager (also known as a backup resource manager). The replica resource manager is then available for retrieval and update in case the primary resource manager is unavailable. When the primary resource manager is again available, it synchronizes with the replica.

Requirement: IBM Content Manager has a maximum limit of 2 GB for the object size that it can replicate. The replicator does not replicate any object larger than 2 GB.

Objects are replicated as they are stored. If the replication fails, for example because of a network outage, then the next attempt to replicate the object will be according to the replication schedule of the resource manager.

You can define your options for replication when you define a resource manager configuration in the New Resource Manager Configuration window of the system administration client. On the Replicator Schedule page, you can define the replicator schedule to specify when you want the replicator to run. On the Cycles page, you can set the amount of time before the system checks to see if replication is necessary.

Recommendation: Run the replicator during times when there is little server activity.

When you define a resource manager in the New Resource Manager Definition window of the system administration client, you can mark a resource manager as unavailable. You might want to mark a resource manager as unavailable if the server is down or is under maintenance. If you mark the resource manager as unavailable, a client bypasses this server and does not store or retrieve objects on it.

In the Library Server Configuration window, you can set the number of seconds that the library server waits to check for the availability of resource managers. You can also set the number of seconds that the library server waits for a response from the resource manager before considering it to be unavailable.

Replication is not intended to replace normal system backups. It is an additional tool to ease recovery from hardware failures, and other such events.

Turning on replication for objects that have already been stored

Replication is a feature that, when configured, creates replicas of objects as they are stored. You can also manually create replicas of objects that are already stored.

Attempt this process only after backing up your systems. Replicate small batches of objects off the same media to ensure maximum efficiency. At first, you should use this procedure when you are the only system user so that you can monitor the replication rate and determine how many objects you can replicate at a time.

If you plan to enable collections for replication, replicate to the same server, or cross replicate between servers that have collections that contain both primary and replicated parts, make a copy of your current `rmobjects` tables. You can then use this copy to distinguish between primary and replicated objects.

Restriction: This procedure works only for primary objects. It is not possible to tell only from resource manager data if an object is a primary or replica object. You must be able to use some group of attributes to determine which objects you have replicated and which objects are primary objects that have yet to be replicated.

Recommendations:

- Make target collections accept replicated data and keep that replicated data separate from primary copies.
- Determine which objects to replicate.
- Choose the target resource manager and target collection on the target server.
- Allow for storage space on the target server.
- Ensure that the space exists for the DB2 tables and logs.
- For remote migration, have entries for the remote resource managers.

Important: Do not allow objects that are being replicated by this process to be discarded until replication is complete. Otherwise you might have requests to replicate objects that do not exist. This problem can result in replication being unable to process these records. If this problem happens, the records need to be identified and removed by hand from the `rmreplication` table.

To manually enable existing objects for replication:

1. Run the migrator. If you have objects of status S, U, or D, the migrator has not completed its work. Do not attempt to replicate.
2. Run the replicator twice. The `rmreplication` table should be empty.
3. Back up the entire system including the library server and both source and target resource managers.
4. On the source resource manager, open a DB2 command prompt.
5. At the DB2 command prompt, connect to the source resource manager database.
6. Determine the distribution of objects by collection. Enter the following query to get a collection and volume distribution:

```
select col_collname, obj_volumeid,
       count(*) from rmobjects a, rmcollections b
       where a.obj_collectionid = b.col_collid and obj_status = 'A'
       group by col_collname, obj_volumeid
       order by col_collname, obj_volumeid
```
7. Enter the following query to get a collection, volume, and date distribution substituting the `SOURCE_COLLECTION` name that you want to replicate. Select a collection, volume, and date range to replicate. For the first time, keep the number small. You might increase the numbers after you are certain that things are set up and working correctly.

```
select col_collname, obj_volumeid, DATE(obj_createdate),
count(*) from rmlibobjects a, rmlibcollections b
where a.obj_collectionid = b.col_collid and obj_status = 'A'
and b.col_collname = 'SOURCE_COLLECTION'
group by col_collname, obj_volumeid ,DATE(obj_createdate)
order by col_collname, obj_volumeid ,DATE(obj_createdate)
```

8. Run the insert action that places the request that replicates the chosen objects.

```
insert into rmlibreplication
select obj_libraryid, obj_itemid, obj_version, obj_collectionid ,
'TARGET.COLL' , b.svr_serverid , 'N' , obj_size ,obj_updatedate,0
from rmlibobjects a, rmlibserver b
where b.svr_servername = 'TARGETRM' and obj_status = 'A'
and obj_volumeid = 1 and obj_createdate between
'2003-01-01-00.00.00.000000' and '2003-01-30-00.00.00.000000'
```

TARGETRM

Target resource manager database name (in uppercase letters).

TARGET.COLL

Target resource manager collection (in uppercase letters).

- 1 Volume that you have selected.

Object creation dates

Replace the timestamp values with the date range that you selected, using the format shown in the example. Use the date format compatible with your database.

If you make a spelling error you might need to remove the problem rows from rmlibreplication. If you leave rows that cannot be processed, the replicator might not function correctly.

9. Enter:

```
select count(*) from rmlibreplication
```

10. Run the replicator. The replicator starts by updating the library server. The rmlibreplication table then has a REP_REPLICATIONTYPE of 'R'. The objects should begin to store on the target server.
11. Verify that the parts have arrived at the target server and that the rmlibreplication table is empty.

Defining replication rules in administrative domains

When administrative domains are enabled in the content management system, the administrative domains affect how replication can be enabled.

For a user to enable replication, the source and target resource managers and collections must be in the user's own domain or the PUBLIC domain. If the user is in the super domain, the user can define a replication rule in any domain. However, the source and target must be in the same domain or one of them must be in the PUBLIC domain.

Library server monitor fail-over service

IBM Content Manager provides a fail-over service that verifies that resource managers are available. If you are trying to store objects into a resource manager that is unavailable, IBM Content Manager tries to store into the next available resource manager. Without this fail-over service, you get an error if you tried to store objects in a resource manager that was unavailable.

Attention: Make sure the resource manager has been started before starting this service.

The fail-over service monitors the availability of the resource managers based on the interval that you set in the Library Server Configuration window. For example, if you set 60 seconds as the interval, it checks availability every 60 seconds. This service should remain running. The library server monitor service is named ICMPLSAP (portable library server asynchronous process) if you are using DB2. If you are using Oracle, use ICMORLSAP. To check whether the service has started, complete one of the following steps:

- On UNIX, make sure that `icmplsap` or `icmorlsap` is running.
- On Windows, check the Services window. The service is called ICM LS monitor (*database name*).

Tip: Stop this service before removing a resource manager from the library server. If the service is running when you remove a resource manager from the library server, log entries will continue to be made indicating that the resource manager is not available. Restarting the service will stop the continuing entries.

Cataloging objects from your local system

When you catalog resource manager objects, you store them on your local system. By using the catalog API, you can instruct the resource manager to turn a directory on your system into another accessible volume.

To catalog objects, you must complete the following steps:

1. Enable the IBM Catalog Device Manager:
 - a. Right-click **Device Managers**.
 - b. Click **New**.
 - c. Type ICMFILEPATH in the **Name** field.
 - d. Click **Enable**.
 - e. Click **OK**.
2. Create a storage class for cataloging, specifying ICMFILEPATH as the device manager.
3. Create a migration policy for cataloging. Add your storage class to it.
4. Create a storage system.
5. Create a storage group.
6. Create a collection for cataloging, specifying your migration policy.
7. Write a program that creates an object and catalogs it. For example:
 - a. Create a text resource item type (Journal) with attributes (Title, Year).

```
DKItemTypeDefICM textItemType = new DKItemTypeDefICM(datastore);
textItemType.setName("Journal");
textItemType.setClassification
(DKConstantICM.DK_ICM_ITEMTYPE_CLASS_RESOURCE_ITEM);
textItemType.setXDOClassId(DKConstantICM.DK_ICM_XDO_TEXT_CLASS_ID);

//add attrs to the item type.
textItemType.addAttr(TitleAttrObj);
textItemType.addAttr(YearAttrObj);
textItemType.add();
```
 - b. Create a resource item and catalog content. For example, to catalog the file `ReadMe.txt` located in `c:\winnt` existing on the resource manager, enter:

```
DKLobICM lob = datastore.createDDO("Journal",DKConstant.DK_CM_ITEM);
lob.catalogContent("ReadMe.txt","c:\winnt");
```

Backing up and restoring your data

To back up and restore data on the resource manager, you can use Tivoli Storage Manager or any other backup utility that is available on your system.

To back up the databases for the servers, use the utilities that are provided with your database software.

Make sure that you back up all components of the IBM Content Manager system together. If you need to restore the system later, each component must be from the same point in time.

1. Identify the LBOSDATA areas. Run the appropriate query for your operating system:

UNIX

```
select vol_mountpoint from rmvolumes
```

Windows

```
select vol_logicalname from rmvolumes
```

2. Pause the system.
3. Back up the following components:
 - Library server database
 - Resource manager database
 - LBOSDATA areas
 - Data stored in Tivoli Storage Manager
4. Resume the system.

Pausing IBM Content Manager for backups

The library server `PAUSESERVER` utility enables you to stop all IBM Content Manager transaction processing in preparation for library server and resource manager backup processes.

To pause IBM Content Manager, run `PAUSESERVER`, specifying a future time (UTC). When the system time is equal to or greater than the time that you specify, the library server will block all new transactions.

If there are transactions processing when the pause time is reached, those transactions will run until completion if they do not exceed the `MAXTXDURATION`. If a transaction that is processing exceeds the maximum time allowed, it is cancelled and all work owned by the transaction is rolled back.

When all transactions have completed on the library server, there will be no client-initiated actions to any resource manager, thereby suspending IBM Content Manager and leaving you free to create a consistent backup of all IBM Content Manager servers.

To pause the library server, follow these steps:

1. Open a DB2 command prompt.
2. Change to the `IBMCMROOT\bin` directory.
3. Enter the version of the command for your operating system:

UNIX

```
./pauseserver.sh dbname userid password SUSPENDSEVERTIME
```

Windows

```
pauseserver.bat dbname userid password SUSPENDSEVERTIME
```

Attention: You can run PAUSESERVER to pause a library server on UNIX, Windows, or z/OS. The only limitation is that the database must be cataloged on the system where you enter the command. For a library server that is located on a remote system, use the local alias in place of the *dbname* variable in the command.

This command updates the SUSPENDSEVERTIME field in the ICMSTYSYSCONTROL table. When that time is less than or equal to the current time, all new transactions are rejected. If an application is storing an object to a resource manager, those operations will complete if they can do so within the time specified in MAXTXDURATION in ICMSTYSYSCONTROL. After that time, all requests to the library server are rejected.

Resuming IBM Content Manager after backups

The RESUMESERVER utility enables you to resume transaction processing. To resume IBM Content Manager, run RESUMESERVER, which will update SUSPENDSEVERTIME to null and resume transaction processing.

To resume library server processing, follow these steps:

1. Open a DB2 command prompt.
2. Change to the *IBMCMROOT\bin* directory.
3. Enter the version of the command for your operating system:

UNIX

```
./resumeserver.sh dbname userid password
```

Windows

```
resumeserver.bat dbname userid password
```

Attention: You can run RESUMESERVER to resume a library server on UNIX, Windows, or z/OS. The only limitation is that the database must be cataloged on the system where you enter the command. For a library server that is located on a remote system, use the local alias in place of the *dbname* variable in the command.

Managing servers in IBM Content Manager

You must maintain the quality and integrity of the system. To maintain the system, your responsibilities include:

- Starting and stopping servers
- Synchronizing servers
- Running the asynchronous recovery utility
- Backing up and restoring your data
- Tracing errors
- Replacing or repartitioning a hard disk

Some of these responsibilities require that you work with your database administrator.

“Starting and stopping a resource manager”

“Resource manager startup behavior” on page 375

“Changing ownership of the resource manager” on page 376

“Starting and stopping resource manager services” on page 376

“Finding data discrepancies with the validation utility” on page 377

“IBM Content Manager data validation utility for z/OS” on page 393

“Managing databases” on page 394

“Optimizing server databases” on page 395

“Logging and tracing for IBM Content Manager” on page 396

Starting and stopping a resource manager

You might find that you have to restart your resource manager. Reasons to restart your resource manager include:

- Picking up changes that you made to the WebSphere Business Integration Server Foundation or WebSphere Application Server configuration file
- Stopping a server from dumping a large amount of data in an abnormal termination
- Installing a new Web archive (WAR) file

Tip: Consolidate changes to minimize downtime caused by restarting your resource manager application server.

“Starting and stopping a resource manager on AIX”

“Starting and stopping a resource manager on Linux” on page 372

“Starting and stopping a resource manager on Solaris” on page 373

“Starting and stopping a resource manager on Windows” on page 374

“Starting and stopping the HTTP server that runs the z/OS resource manager” on page 375

Starting and stopping a resource manager on AIX

You might have to start and stop a resource manager to complete maintenance or troubleshooting tasks.

You must be logged in to the WebSphere Business Integration Server Foundation or WebSphere Application Server system to use the following commands. In a default installation, the commands are located in `/usr/WebSphere/AppServer/profiles/RM_PROFILE/bin`. `RM_PROFILE` indicates the WebSphere Application Server profile name where the resource manager application server is deployed.

Attention: WebSphere Business Integration Server Foundation or WebSphere Application Server might be configured to permit non-root user IDs to run application servers. If it is not set up to permit this, you must be logged in as the root user to start, stop, or check the status of the resource manager application server.

Requirement: If the system is configured to use the IBM HTTP Server in conjunction with WebSphere Business Integration Server Foundation or WebSphere Application Server, the HTTP server must be started.

- To check the status of the resource manager application server, enter:
`./serverStatus.sh server1`
- To start the resource manager application server, enter the following commands, each on a separate line:
`./home/db2inst1/sqllib/db2profile`
`./startServer.sh server1`

To make sure that the resource manager application server has started, you can:

- View the output of the `startServer` command. The message "Server *server1* open for e-business" indicates that your resource manager application server was started successfully.
 - Look in `startServer.log` for the line:
Server *server1* open for e-business
Logs are written in the `/usr/WebSphere/AppServer/profiles/RM_PROFILE/logs/server1` directory.
 - Use the `serverStatus` command.
- To stop the resource manager application server, enter:
`./stopServer.sh server1`

Starting and stopping a resource manager on Linux

You might have to start and stop a resource manager to complete maintenance or troubleshooting tasks.

You must be logged in to the WebSphere Business Integration Server Foundation or WebSphere Application Server system to use the following commands. In a default installation, the commands are located in `/opt/WebSphere/AppServer/profiles/RM_PROFILE/bin`. `RM_PROFILE` indicates the WebSphere Application Server profile name where the resource manager application server is deployed.

Attention: WebSphere Business Integration Server Foundation or WebSphere Application Server might be configured to permit non-root user IDs to run application servers. If it is not set up to permit this, you must be logged in as the root user to start, stop, or check the status of the resource manager application server.

Requirement: If the system is configured to use the IBM HTTP Server in conjunction with WebSphere Business Integration Server Foundation or WebSphere Application Server, the HTTP server must be started.

- To check the status of the resource manager application server, enter:
`./serverStatus.sh server1`
 - To start the resource manager application server, enter the following commands, each on a separate line:
`./home/db2inst1/sqllib/db2profile`
`./startServer.sh server1`
- To make sure that the resource manager application server has started, you can:
- View the output of the startServer command. The message "Server *server1* open for e-business" indicates that your resource manager application server was started successfully.
 - Look in startServer.log for the line:
Server *server1* open for e-business
Logs are written in the /opt/WebSphere/AppServer/profiles/RM_PROFILE/logs/*server1* directory.
 - Use the serverStatus command.
- To stop the resource manager application server, enter:
`./stopServer.sh server1`

Starting and stopping a resource manager on Solaris

You might have to start and stop a resource manager to complete maintenance or troubleshooting tasks.

You must be logged in to the WebSphere Business Integration Server Foundation or WebSphere Application Server system to use the following commands. In a default installation, the commands are located in /opt/WebSphere/AppServer/profiles/RM_PROFILE/bin. RM_PROFILE indicates the WebSphere Application Server profile name where the resource manager application server is deployed.

Attention: WebSphere Business Integration Server Foundation or WebSphere Application Server might be configured to permit non-root user IDs to run application servers. If it is not set up to permit this, you must be logged in as the root user to start, stop, or check the status of the resource manager application server.

- To check the status of the resource manager application server, enter:
`./serverStatus.sh server1`
- To start the resource manager application server, enter the following commands, each on a separate line:
`./export/home/db2inst1/sqllib/db2profile`
`./startServer.sh server1`

To make sure that the resource manager application server has started, you can:

- View the output of the startServer command. The message "Server *server1* open for e-business" indicates that your resource manager application server was started successfully.
 - Look in startServer.log for the line:
Server *server1* open for e-business
Logs are written in the /opt/WebSphere/AppServer/logs/profiles/RM_PROFILE/logs/*server1* directory.
 - Use the serverStatus command.
- To stop the resource manager application server, enter:


```
./stopServer.sh server1
```

Starting and stopping a resource manager on Windows

You might have to start and stop a resource manager to complete maintenance or troubleshooting tasks.

You must be logged in to the WebSphere Business Integration Server Foundation or WebSphere Application Server system to use the following commands. In a default installation, the commands are located in the `c:\Program Files\IBM\WebSphere\AppServer\profiles\RM_PROFILE\bin\` path. `RM_PROFILE` indicates the WebSphere Application Server profile name where the resource manager application server is deployed. Execute each one from a command prompt.

Requirement: If the system is configured to use the IBM HTTP Server with WebSphere Business Integration Server Foundation or WebSphere Application Server, the HTTP server must be started.

Tip: To start the resource manager application server automatically as a Windows service, use the **WASService** command. See the WebSphere Application Server Information Center for the **WASService** command syntax. If you start the resource manager application as a Windows service, you should stop it the same way.

Systems that include storage area networks (SANs) or network-attached storage (NAS), however, require the resource manager to be started from the command line.

- To check the status of the resource manager application server, enter the following command:
`serverStatus server1`
- To start the resource manager application server from the command line, enter the following command:
`startServer server1`

To make sure that the resource manager application server has started, you can check the following data:

- View the output of the `startServer` command.
- Look in `c:\Program Files\IBM\WebSphere\AppServer\profiles\RM_PROFILE\logs\server1\startServer.log` for the line:
`Server server1 open for e-business`
- Use the `serverStatus` command.

Important: A system-wide event, such as user logoff, stops the resource manager if it was started from the command line. Whenever possible, start the resource manager using the **WASService** command.

- To stop the resource manager application server, enter:
`stopServer server1`

Related information

 WebSphere Application Server Information Center

Starting and stopping the HTTP server that runs the z/OS resource manager

You might have to start and stop a resource manager to complete maintenance or troubleshooting tasks.

You do not start or stop the z/OS resource manager, but you can start and stop the HTTP Server that runs it. The HTTP Server for z/OS is a JCL procedure. It usually resides in your proclib, and is started from SDSF with the **START** command. Likewise, it can be stopped in SDSF with the **STOP** command.

You can also stop the z/OS resource manager in the system administration client. Doing this procedure does not stop the resource manager, but the library server considers it unavailable. To stop the z/OS resource manager from the system administration client:

1. Right-click the server name, and click **Properties**.
2. In the Properties window, select the **Server is unavailable** check box. After you select this check box, the library server treats this resource manager as if it is offline and routes clients to an existing replica.

Resource manager startup behavior

When you start a resource manager, you should be aware of startup behaviors that affect the startup process and subsequent restarts of the resource manager.

When the resource manager starts, it checks the PROPERTYNAME column in the resource manager database table RMCONFIGURATION for the **ICMRM_USER** parameter and its value. If there is no value set for the **ICMRM_USER** parameter, the resource manager sets this value from the current system user name by using the Java system variable `user.name`. If the value is set, the property value is compared to the Java system variable `user.name`. If these values are not equal, the resource manager exits the startup sequence and returns the ICM9880 unrecoverable error.

The purpose of this behavior is to prevent the resource manager from writing object files with two different owners. The purpose is also to prevent the resource manager from being unable to access previously written object files. In addition, this behavior also allows the resource manager process to be configured without side effects on the other processes of the resource manager process owner.

Important: If you change the user name that runs the resource manager, the resource manager cannot start unless you complete the steps to change the owner of the resource manager application server. For a UNIX system, you must then change the ownership of the resource manager object files. You must make this change so that the new owner of the resource manager application server can access object files stored by the previous resource manager application server owner.

Changing ownership of the resource manager

If you want to change the ownership of a resource manager application server, you must complete tasks to ensure that the new owner can start the resource manager and that the files on that resource manager are accessible. You must also consider other factors that affect the ability to access files on that resource manager.

You can change the ownership of a resource manager application server by changing the value for the **ICMRM_USER** parameter, the resource manager user in the RMCONFIGURATION resource manager table. When you change the owner of the resource manager, you must also consider how a change to the resource manager owner affects files on that resource manager and the WebSphere Application Server installation. For the UNIX operating system, you must change ownership of the resource manager object files to the new owner to enable the resource manager to access object files stored with the previous owner's user name. Because the owner of the resource manager is also the user that runs WebSphere Application Server, you must also change the user that runs WebSphere Application Server.

If your content management system includes stored objects on Tivoli Storage Manager, changing the ownership of a resource manager can be problematic. After you change the ownership of the resource manager and the resource manager is restarted, the object files stored on Tivoli Storage Manager with the previous resource manager owner are not accessible by the changed owner.

Recommendation: If your content management system includes stored objects on Tivoli Storage Manager, changing the ownership of the resource manager is not recommended.

To change the ownership of a resource manager application server:

1. Stop the resource manager application server.
2. Edit the RMCONFIGURATION resource manager table and modify the value of the **ICMRM_USER** parameter to the Java system variable *user.name* of the new owner.
3. For UNIX, change the ownership of all resource manager object files to the user name of the new resource manager owner by using the **chown** command. Run the command recursively on each top-level file system that contains resource manager objects.
4. Start the resource manager application server again by using the new user name for the resource manager.

Related reference
RMCONFIGURATION

Starting and stopping resource manager services

You can start and stop the resource manager services by using the system administration client.

To start or stop resource manager services, you must be logged in to the system administration client.

1. In the system administration client tree view, click **Resource Managers** and click the resource manager you want to work with.
2. Click **Configurations** in the tree view, then click **IBMCONFIG**.
3. Click **Services** and then click the appropriate start or stop button.

Finding data discrepancies with the validation utility

Use the validation utility to find data discrepancies between the library server and the resource manager and between the resource manager and the storage systems.

You run the validation utility by using the resource manager administration console, a tool that is used to perform some of the maintenance tasks for a resource manager.

Tip: You can also create a custom application that uses the IBM Content Manager APIs to run the validation utility with a schedule that you define.

To open the resource manager administration console and set up and run the validation utility:

1. Enter the web address for the resource manager administration console:

`https://RM_Hostname:HTTPS_Port/resource_manager/admin`

where *RM_Hostname* is the host name for the resource manager, *HTTPS_Port* is the port for the resource manager application, and *resource_manager* is the name of the resource manager.

2. Log in with the administrator user ID and password for the resource manager.
3. Click the **Validator** tab to open the Validator page.
4. Enter the date range for the data that you want to check in the **Begin Date** and **End Date** fields, in the format *YYYY-MM-DD-hh.mm.ss*. The date range fields are optional. If a **Begin Date** value is not provided but an **End Date** value is provided, all objects with time stamps earlier than the **End Date** value are checked. If a **Begin Date** value is provided and an **End Date** value is not provided, all objects with time stamps from the **Begin Date** value to the time that the validator runs are checked. If the **Begin Date** and the **End Date** are both not provided, all of the objects are checked. All date and time elements are required in the entry, but a 0 value can be used for the time elements. For the date elements, *YYYY* is the value for the year, *MM* is the value for the month, *DD* is the value for the day. For the time elements, *hh* is the value for the hour based on a 24-hour clock, *mm* is the value for the minute, and *ss* is the value for the second. A 0 value can be used for the time elements.
5. To define the types of data checked by the validation utility, select values in the **Storage Volumes** and the **Metadata** fields.

Option	Description
Check discrepancies between the resource manager and the storage volume	Select all to check all storage volumes or select a specific volume. If you do not want the validation utility to check this type of data, select none .

Option	Description
Check discrepancies between the resource manager and the library server	Select all to check data in both the resource manager and library server production system and the RMMIGRATIONTASKS table. Select RMOBJECTS to check data in the library server and resource manager production system only. Select RMMIGRATIONTASKS to check data in the RMMIGRATIONTASKS table only. If you do not want the validation utility to check this type of data, select none .

6. Click **Start** to run the validation utility. You can view information about the progress of the utility on the Validator page. The information includes the current validation step, the estimated number of objects to be checked, and the number of objects retrieved and processed.
7. Click the **Validation Report** tab to view the validation utility discrepancy report.
 - “Resource manager validation utilities”
 - “Validation utility discrepancy reports”
 - “Saving validation utility discrepancy reports as XML files” on page 380
 - “Using the APIs for validation utility scheduling” on page 381
 - “Repairing data discrepancies with the validation utility recovery tools” on page 383

Resource manager validation utilities

The validation utilities analyze discrepancies among three components: the library server, the resource manager, and the storage systems used by the resource manager through its defined device managers.

Any of the components can fail and require a restoration from a backup that can be unsynchronized with the other two components. Examples of storage systems are DB2 Content Manager VideoCharger or Tivoli Storage Manager.

Because there is no direct link between the library server and the storage system, differences must be reported between the library server and the resource manager and between the resource manager and the storage system. The validation utility generates reports that describe discrepancies between the library server and the resource manager and discrepancies between the resource manager and the storage system. The reports are stored in the resource manager database in the RMVALREPORT table. You can use commonly available database tools or the resource manager administration console to view the reports. You can also optionally save the reports as XML files.

Restriction: Run the validation utilities when the resource manager is offline or at an off-peak time to improve the accuracy of the reports. If the resource manager is in use while the validation utilities are running, inaccurate synchronization errors might be reported.

Validation utility discrepancy reports

The validation utility provides reports that contain the error types that are found by the utility. You can view the reports in several ways.

You can view the report data in the RMVALREPORT table in the resource manager database, in the resource manager administration console, or in XML files.

Table 68. Viewing options for the validation utility discrepancy reports

Viewing option	Description
As data in the resource manager database RMVALREPORT table	The data that is saved to the RMVALREPORT table is cumulative until the table data is cleared. You can clear the data by using database commands or by clicking Clear Report on the Validation Report page of the resource manager administration console.
As a web-based report from the Validation Report page in the resource manager administration console	The data that is saved to the Validation Report page is cumulative per resource manager administration console session. You can clear the data by clicking Clear Report . This action also clears the report data saved to the RMVALREPORT table.
As an XML file	If you set a path as the value for the VALIDATION_XML_LOGPATH parameter, then each time that you run the validation utility, the report information saves as XML files with unique names and time stamps. Each type of error report, such as ORPHAN or NOTINRM, saves to a file that you can view. For those error types that have a validation utility recovery tool, you can also use the XML file for the report as the input file for the tool. This option is recommended if you plan to use the validation utility recovery tools.

The following table describes the error types found by the validation utility.

Table 69. Validation utility error type descriptions

Error type	Description
ORPHAN	An object is on the resource manager, but the library server does not have a reference to the object. The report contains information about the object from the resource manager database.
NOTINRM	The library server has a reference to an object, but the object is not on the resource manager. The report contains information about the object from the library server database.
SIZEMISMATCH	The size of an object on the library server does not match the size of the object on the resource manager. The report contains information about the object from the resource manager and library server databases.
COLLECTION	The collection of an object on the library server does not match the collection of the object on the resource manager. The report contains information about the object from the resource manager and library server databases.

Table 69. Validation utility error type descriptions (continued)

Error type	Description
DATEMISMATCH	The object update date on the library server does not match the object update date on the resource manager. Under normal circumstances, if there is any synchronization problem between the library server and the resource manager, the object update date does not match. To reduce redundant entries in the different reports, entries are not added to the DATEMISMATCH report if they are added to the COLLECTION or SIZEMISMATCH reports. The report contains information about the object from the resource manager and library server databases.
FILENOTFOUND	An object is in the resource manager database but it was not found on the volume recorded in the database. A file is considered "not found" if it meets one of the following conditions: <ul style="list-style-type: none"> the device manager of the volume reported that the file did not exist the device manager of the volume reported that the file had a zero file size when the size in the database is nonzero The report contains the object information from the resource manager database.
FILESIZEMISMATCH	The size of an object in the resource manager database does not match the size reported by the device manager. The report contains the object information from the resource manager database and the size reported by the device manager.
ITEMIDINVALID	An item ID from the RMMIGRATIONTASKS table contains a timestamp type format where the item ID starts with a timestamp such as "19" or "20" in the database table. This entry generally results from a problem during the upgrade from Version 8.3 to Version 8.4, when the migration task had pending transactions.
FILEMISPLACED	An object is in the resource manager database, but was not found on the volume recorded in the database. However, the object exists under a null subdirectory. This error condition occurs when the file path for the object on the storage volume was incorrectly created as <i>drive:/null/collection_number/</i> when the correct file path should be <i>drive:/lbosdata/collection_number/</i> , where <i>drive</i> is the drive letter on Windows or the mount point on UNIX and <i>collection_number</i> is the collection number.

Saving validation utility discrepancy reports as XML files

To save the validation utility discrepancy report data as XML files, set a value for the **VALIDATION_XML_LOGPATH** parameter.

Each time that you run the validation utility, the report data saves to the **RMVALREPORT** table. However, the data in this table is cumulative and the table can be cleared to remove the report data.

If you want to preserve the data gathered when you run the validation utility, you can save the data to a set of XML files. Each type of error found during the running of the utility, such as **ORPHAN** or **NOTINRM**, saves to an XML file for that error type. The file saves with a unique name that includes a date stamp and

time stamp as part of the name. The benefits of saving the report data include preserving the validation utility output at a unique moment in time, without cumulative data added from a subsequent running of the utility, being able to view and share the data later for further analysis, and being able to use the data as input for the validation utility recovery tools.

To save the validation utility reports to XML files, set the path where you want the XML files to be saved as the value for the **VALIDATION_XML_LOGPATH** parameter. You can change the value of this parameter from the resource manager administration console or from the RMCONFIGURATION table in the resource manager database.

For example, if you set the value of the **VALIDATION_XML_LOGPATH** to C:\temp, and you ran the validation utility on September 7, 2010, and the validation utility found ORPHAN and NOTINRM errors, and the files saved at 12:19:57, the following XML files that contain validation utility discrepancy report data would be created:

- C:\temp\icmrm\sva\20100907121957_ORPHAN.xml
- C:\temp\icmrm\sva\20100907121957_NOTINRM.xml

To save the validation utility reports as XML files from the resource manager administration console:

1. Choose one of the following actions:

Option	Description
To set the value from the resource manager administration console	Click the Advanced Parameters tab.
To set the value from the resource manager database	Find the VALIDATION_XML_LOGPATH parameter in the RMCONFIGURATION table.

2. In the **VALIDATION_XML_LOGPATH** field, enter the path where you want to save the validation utility report files. This path must be a local path on the machine where the resource manager administration console is running.

Using the APIs for validation utility scheduling

When you run the validation utility from the resource manager administration console, the utility runs immediately. You cannot schedule when the validation utility runs. To create a schedule for the validation utility, you must develop your own application that uses the IBM Content Manager Java APIs.

By using the functions defined in the APIs, you can create an application that can start, stop, schedule, and monitor the validation utility. The schedule and options that you assign in your application persist in the resource manager database. For example, you can create an application that assigns a daily or weekly schedule for running the validation utility. After you run the application, that schedule is saved to the resource manager database and runs as defined by the application.

Authorization to run the validation utility from the APIs

The APIs do not require the use of an administrator ID with database authority or administrator privileges on the library server and resource manager. Any user ID that includes the SystemDefineRM privilege can be used to run the validation utility from the APIs. This authorization is different from what is required to run

the validation utility from the resource manager administration console. From the console, the utility must be run with the administrator ID for the resource manager.

Options and requirements for scheduling the validation utility

From your custom application, you can schedule the validation utility to run once immediately, run once at a scheduled time, or run repeatedly on a schedule that you define. When your application runs, the schedule data is persisted on the resource manager database.

The option to run the validation utility immediately is controlled in the API by the `setValidationRunImmediate` method that accepts a Boolean input such as `true` or `false`. If you have an active schedule for the validation utility saved to a resource manager and then you run your application again with the option set to run immediately, this setting ignores any schedule that is saved to the resource manager database. You must run your application again with the option to run immediately set to `false` to reactivate your schedule.

When you set a schedule for the validation utility, you must define a start time and a duration time. This start time and duration time is similar to the start time and duration time set on other resource manager services such as the replicator and migrator. However, unlike replicator and migrator services, the validation utility cannot be resumed if it is stopped. If the validation utility is stopped prematurely and does not complete all validation operations, then the report data contains output that the report is incomplete. A premature stop of the validation utility might occur if the validation utility is stopped manually or the validation utility activity exceeds the duration time.

You can use your application to stop an active schedule or a validation that is currently running. However, some validation operations cannot be interrupted and must continue until they are complete. Therefore, if the duration time expires or if you stop the validation utility while it is running, the operation that is currently running completes and then the validation utility is stopped.

Only one instance of the validation utility can be active at one time on a resource manager. For example, if a schedule set up through the APIs is active, then you cannot use the resource manager administration console to run the web-based version of the validation utility. Similarly, if you are currently running the validation utility from the resource manager administration console, then you cannot schedule the validation utility to run by starting your application that uses the APIs. In addition, if you start the validation utility from the APIs, then you cannot start it again from the APIs without stopping it first. If the validation utility is running either from the APIs or from the resource manager administration console, shared information that is available from both the console and the API status operation does indicate if the validation utility service is active.

As with the validation utility that runs from the resource manager administration console, you can choose to save the validation reports as XML files. The XML files can be used as input for the validation recovery tools. To save the validation reports as XML files, you must supply a path for the `VALIDATION_XML_LOGPATH` parameter. This parameter is in the `RMCONFIGURATION` table in the resource manager database. The APIs use the value that is saved to the `VALIDATION_XML_LOGPATH` parameter. You cannot supply a value for this parameter directly through the APIs.

Where to find more information about creating your application with the APIs

For more information about creating your own application that uses the APIs to run the validation utility, see the documentation for these APIs in the *Application Programming Reference*. See also the sample API code.

Related tasks

“Saving validation utility discrepancy reports as XML files” on page 380

Related reference

 Sample to demonstrate the use of Content Manager EE APIs to schedule and run the validation utility

Javadoc: Package com.ibm.mm.sdk.rm

Repairing data discrepancies with the validation utility recovery tools

You can use the validation utility recovery tools to repair some of the data discrepancies that occur between the library server and the resource manager and between the resource manager and the storage systems.

“Setting up the validation utility recovery tools”

“Repairing FILENOTFOUND errors with the ICMFILENOTFOUNDCleanup recovery tool” on page 384

“Repairing NOTINRM errors with the ICMNOTINRMCleanup recovery tool” on page 386

“Repairing ORPHAN errors with the ICMORPHANCleanup recovery tool” on page 389

“Repairing ITEMIDINVALID errors with the ICMITEMIDINVALIDCleanup recovery tool” on page 391

Setting up the validation utility recovery tools

To run the validation utility recovery tools, you must configure the client API environment on a machine that has access to both the library server and the resource manager.

The validation utility recovery tools are available as part of the code for the system administration client. You can find the validation utility recovery tools in `%IBMCMROOT%\admin\rmtools`, where `%IBMCMROOT%` is the installation path for the system administration client. For example, for Windows, the default path for `%IBMCMROOT%` is `C:\Program Files\IBM\db2cmv8` and the default path for UNIX is `/opt/IBM/db2cmv8`.

To set up the validation utility recovery tools, complete the following steps from a machine with connectivity to both the library server and the resource manager:

1. Set up the client API environment by running the appropriate command for your operating system.

Option	Description
Windows	<code>%IBMCMROOT%\bin\cmbenv81.bat</code>
UNIX	<code>%IBMCMROOT%/bin/cmbenv81.sh</code>

2. Set the system CLASSPATH environment variable to contain the path to the JDBC JAR files for DB2 or Oracle.

Repairing FILENOTFOUND errors with the ICMFILENOTFOUNDCleanup recovery tool

You run the ICMFILENOTFOUNDCleanup validation utility recovery tool to fix FILENOTFOUND errors reported by the validation utility.

Before you run the validation utility recovery tools, back up your library server and resource manager databases. There is no utility to reverse the changes that are made to the databases by the recovery tools.

If the resource manager server has a reference to an object but the object is not on the resource manager server volume, then the resource manager volume validation utility identifies and flags this object with a FILENOTFOUND error in the RMVALREPORT table. The ICMFILENOTFOUNDCleanup validation utility recovery tool removes metadata from both the library server database and the resource manager database to repair this error condition.

Remember: The example commands in the following procedure are shown on multiple lines to improve readability. Enter the commands on a single line.

To run the ICMFILENOTFOUNDCleanup validation utility recovery tool:

1. Run the validation utility to generate the report data for the validation utility recovery tool.
2. Optional: Run the ICMFILENOTFOUNDCleanup recovery tool with no parameters to ensure that the API client environment is configured correctly and to view the help for all parameters. For example:

```
java -cp ICMFileNotFoundCleanup.jar;%CLASSPATH%
com.ibm.cm.rmtools.ICMFILENOTFOUNDCleanup
```

This command returns the following usage information for the ICMFILENOTFOUNDCleanup validation utility recovery tool:

ERROR: Missing input parameters

Usage:

```
java -cp ICMFILENOTFOUNDCleanup.jar;%CLASSPATH%
com.ibm.cm.rmtools.ICMFILENOTFOUNDCleanup
    -lsName
    -lsUserid
    -lsPassword
    -rmName <db2name or oracle service name>
    -rmUserid
    -rmPassword
    -rmHost
    -dbType <db2/oracle>
    -dbPort <database port number>
    -dbSchema <database schema>
    -pf <FILENOTFOUND xml file>
    -task <task number>
    -noprompt (Optional) Add this parameter to delete
    items without prompting for confirmation
    -batchsize <delete batch size>
```

where:

lsName	- Library server database name
lsUserid	- Library server administrator id
lsPassword	- Library server administrators password
rmName	- Resource manager database name <db2>
	or service name <oracle>
rmUserid	- Resource manager administrator id

rmPassword	- Resource manager administrator's password
rmHost	- Resource manager host name
dbType	- Type of Database - i.e. db2 or oracle
dbPort	- Database port number (i.e. 50000 for db2, 1521 for Oracle)
dbSchema	- Database schema (i.e. RMADMIN)
pf	- Name of Content Manager Validation Utility *FILENOTFOUND.xml file
task	- The task to be executed Available tasks are: 1 - Find items 2 - Retrieve and Display Items 3 - Delete Items
noprompt	- Add this parameter to delete items without prompting for confirmation
batchsize	- Add this parameter to delete items in batches (default is 500 items per batch)

Tip: An error message that is similar to the following message indicates that the environment is not set up correctly on the machine where you are running the validation utility recovery tool:

The java class is not found: com/ibm/mm/sdk/common/dkCollection

If you receive this message, complete the steps to set up the validation utility recovery tools.

- Decide if you want to run the validation utility recovery tool against the error report data in the RMVALREPORT table or the error report data in a saved XML report (if applicable).

Option	Description
Run the recovery tool against the data in the RMVALREPORT table	<p>When you run the recovery tool against the data in the RMVALREPORT table, you must supply information about the database as values for the dbType, dbPort, and dbSchema parameters.</p> <p>Running the recovery tool against the data in the database means that you could be running the tool against older, cumulative report data or that expected report data could be missing if the RMVALREPORT data was manually cleared.</p>
Run the recovery tool against the data in a saved XML report	<p>If you configured the VALIDATION_XML_LOGPATH parameter to save validation utility report data as XML files, then when you run the recovery tool against the data in a saved XML report, you must supply the file name of the XML report file as a value for the pf parameter. The dbType, dbPort, and dbSchema parameters to supply information about the database are optional.</p> <p>Running the recovery tool against the data in the XML report file means that you are running the recovery tool against one set of error report data collected from a single scan by the validation utility.</p>

For the remainder of this procedure, the examples are shown with a choice to run the validation utility recovery tool against an XML file.

4. Run the ICMFILENOTFOUNDcleanup validation utility recovery tool in retrieve mode, with the **task** parameter set to a value of 2, to retrieve and display the affected objects. The following example shows how to run the command in the retrieve mode:

```
java -cp ICMFILENOTFOUNDcleanup.jar;%CLASSPATH%
com.ibm.cm.rmtools.ICMFILENOTFOUNDcleanup
-lsName icmnlbdb -lsUserid icmadmin -lsPassword ce4win
-rmName rmdb.example.com -rmUserid rmdadmin -rmPassword ce4win
-rmHost cmi375.example.com
-pf C:\temp\icmrmlsval20100907121957_FILENOTFOUND.xml -task 2
```

5. Run the ICMFILENOTFOUNDcleanup validation utility recovery tool in delete mode, with the **task** parameter set to a value of 3, to delete the metadata for the objects on the library server and resource manager. The following example shows how to run the command in delete mode where objects are deleted in batches of 20:

```
java -cp ICMFILENOTFOUNDcleanup.jar;%CLASSPATH%
com.ibm.cm.rmtools.ICMFILENOTFOUNDcleanup
-lsName icmnlbdb -lsUserid icmadmin -lsPassword ce4win
-rmName rmdb.example.com -rmUserid rmdadmin -rmPassword ce4win
-rmHost cmi375.example.com
-pf C:\temp\icmrmlsval20100907121957_FILENOTFOUND.xml -task 3 -batchsize 20
```

Because the **noprompt** parameter is not set in this command, the validation utility prompts the user about the action to perform on each batch.

6. Run the ICMFILENOTFOUNDcleanup validation utility recovery tool in retrieve mode again to ensure that all library server and resource manager metadata is removed. For example:

```
java -cp ICMFILENOTFOUNDcleanup.jar;%CLASSPATH%
com.ibm.cm.rmtools.ICMFILENOTFOUNDcleanup
-lsName icmnlbdb -lsUserid icmadmin -lsPassword ce4win
-rmName rmdb.example.com -rmUserid rmdadmin -rmPassword ce4win
-rmHost cmi375.example.com
-pf C:\temp\icmrmlsval20100907121957_FILENOTFOUND.xml -task 2
```

Related tasks

“Setting up the validation utility recovery tools” on page 383

Repairing NOTINRM errors with the ICMNOTINRMcleanup recovery tool

You run the ICMNOTINRMcleanup validation utility recovery tool to fix NOTINRM errors reported by the validation utility.

Before you run the validation utility recovery tools, back up your library server and resource manager databases. There is no utility to reverse the changes that are made to the databases by the recovery tools.

If the library server has a reference to an object, but the object is not found on the resource manager, then the validation utility flags this object with a NOTINRM error in the RMVALREPORT table. The ICMNOTINRMcleanup validation utility recovery tool deletes the library server references to these objects to repair this error condition.

Remember: The example commands in the following procedure are shown on multiple lines to improve readability. Enter the commands on a single line.

To run the ICMNOTINRMcleanup recovery tool:

1. Run the validation utility to generate the report data for the validation utility recovery tool.

2. Optional: Run the ICMNOTINRMCleanup validation utility recovery tool with no parameters to ensure that the API client environment is configured correctly and to view the help for all parameters. For example:

```
java -cp ICMNOTINRMCleanup.jar;%CLASSPATH% com.ibm.cm.rmtools.ICMNOTINRMCleanup
```

This command returns the following usage information for the ICMNOTINRMCleanup validation utility recovery tool:

ERROR: Missing input parameters

Usage:

```
java -cp ICMNOTINRMCleanup.jar;%CLASSPATH% com.ibm.cm.rmtools.ICMNOTINRMCleanup
  -lsName
  -lsUserid
  -lsPassword
  -rmName <db2name or oracle service name>
  -rmUserid
  -rmPassword
  -rmHost
  -dbType <db2/oracle>
  -dbPort <database port number>
  -dbSchema <database schema>
  -pf <NOTINRM xml file>
  -task <task number>
  -noprompt (Optional)
  -deletebatchsize <delete batch size> (Optional)
```

where:

lsName	- Library server database name
lsUserid	- Library server administrator id
lsPassword	- Library server administrators password
rmName	- Resource manager database name <db2> or service name <oracle>
rmUserid	- Resource manager administrator id
rmPassword	- Resource manager administrator's password
rmHost	- Resource manager host name
dbType	- Type of Database - i.e. db2 or oracle
dbPort	- Database port number (i.e. 50000 for db2, 1521 for Oracle)
dbSchema	- Database schema (i.e. RMADMIN)
pf	- Name of Content Manager Validation Utility NOTINRM.xml file
task	- The task to be executed Available tasks are: 1 - Find items 2 - Retrieve and Display Items 3 - Delete Items
noprompt	- Add this parameter to delete items without prompting for confirmation
deletebatchsize	- Add this parameter to delete items in batches (default is 1 item per batch)

Tip: An error message that is similar to the following message indicates that the environment is not set up correctly on the machine where you are running the validation utility recovery tool:

The java class is not found: com/ibm/mm/sdk/common/dkCollection

If you receive this message, complete the steps to set up the validation utility recovery tools.

3. Decide if you want to run the validation utility recovery tool against the error report data in the RMVALREPORT table or the error report data in a saved XML report (if applicable).

Option	Description
Run the recovery tool against the data in the RMVALREPORT table	<p>When you run the recovery tool against the data in the RMVALREPORT table, you must supply information about the database as values for the dbType, dbPort, and dbSchema parameters.</p> <p>Running the recovery tool against the data in the database means that you could be running the tool against older, cumulative report data or that expected report data could be missing if the RMVALREPORT data was manually cleared.</p>
Run the recovery tool against the data in a saved XML report	<p>If you configured the VALIDATION_XML_LOGPATH parameter to save validation utility report data as XML files, then when you run the recovery tool against the data in a saved XML report, you must supply the file name of the XML report file as a value for the pf parameter. The dbType, dbPort, and dbSchema parameters to supply information about the database are optional.</p> <p>Running the recovery tool against the data in the XML report file means that you are running the recovery tool against one set of error report data collected from a single scan by the validation utility.</p>

For the remainder of this procedure, the examples are shown with a choice to run the validation utility recovery tool against an XML file.

- Run the ICMNOTINRMCleanup validation utility recovery tool in retrieve mode, with the **task** parameter set to a value of 2, to retrieve and display the affected objects. The following example shows how to run the command in the retrieve mode:

```
java -cp ICMNOTINRMCleanup.jar;%CLASSPATH% com.ibm.cm.rmtools.ICMNOTINRMCleanup
-lsName icmnlbdb -lsUserid icmadmin -lsPassword ce4win
-rmName rmdb.example.com -rmUserid rmdadmin -rmPassword ce4win
-rmHost cmi375.example.com
-pf C:\temp\icmrmlsval20100907121957_NOTINRM.xml -task 2
```

- Run the ICMNOTINRMCleanup validation utility recovery tool in delete mode, with the **task** parameter set to a value of 3, to delete the library server references to the objects that do not exist on the resource manager. The following example shows how to run the command delete mode where objects are deleted in batches of 10:

```
java -cp ICMNOTINRMCleanup.jar;%CLASSPATH% com.ibm.cm.rmtools.ICMNOTINRMCleanup
-lsName icmnlbdb -lsUserid icmadmin -lsPassword ce4win
-rmName rmdb.example.com -rmUserid rmdadmin -rmPassword ce4win
-rmHost cmi375.example.com
-pf C:\temp\icmrmlsval20100907121957_NOTINRM.xml -task 3 -deletebatchsize 10
```

Because the **noprompt** parameter is not set in this command, the validation utility prompts the user about the action to perform on each batch.

- Run the ICMNOTINRMCleanup validation utility recovery tool in retrieve mode again to ensure that all the library server references are removed. For example:

```
java -cp ICMNOTINRMCleanup.jar;%CLASSPATH% com.ibm.cm.rmtools.ICMNOTINRMCleanup
-lsName icmnlldb -lsUserid icmadmin -lsPassword ce4win
-rmName rmdb.example.com -rmUserid rmdadmin -rmPassword ce4win
-rmHost cmi375.example.com
-pf C:\temp\icmrmlsval20100907121957_NOTINRM.xml -task 2
```

Related tasks

“Setting up the validation utility recovery tools” on page 383

Repairing ORPHAN errors with the ICMORPHANCleanup recovery tool

You run the ICMORPHANCleanup validation utility recovery tool to fix ORPHAN errors reported by the validation utility.

Before you run the validation utility recovery tools, back up your library server and resource manager databases. There is no utility to reverse the changes that are made to the databases by the recovery tools.

If an object is in the resource manager database, but the library server does not have a reference to the object, then the validation utility flags this object with an ORPHAN error in the RMVALREPORT table. The ICMORPHANCleanup validation utility recovery tool creates an SQL script to mark these orphan items with a D flag in the OBJ_STATUS column of the RMOBJECTS database table. When the SQL script runs against the resource manager, the resource manager migrator service processes the objects marked with the D flag and initiates delete processing. The objects are deleted from the RMOBJECTS database table and from the storage volume and the space is reclaimed.

Remember: The example commands in the following procedure are shown on multiple lines to improve readability. Enter the commands on a single line.

To run the ICMORPHANCleanup validation utility recovery tool:

1. Run the validation utility to generate the report data for the validation utility recovery tool.
2. Optional: Run the ICMORPHANCleanup recovery tool with no parameters to ensure that the API client environment is configured correctly and to view the help for all parameters. For example:

```
java -cp ICMORPHANCleanup.jar;%CLASSPATH% com.ibm.cm.rmtools.ICMORPHANCleanup
```

This command returns the following usage information for the ICMORPHANCleanup validation utility recovery tool:

```
ERROR: Missing input parameters
```

Usage:

```
java -cp ICMORPHANCleanup.jar;%CLASSPATH% com.ibm.cm.rmtools.ICMORPHANCleanup
-rmName <db2name or oracle service name>
-rmUserid
-rmPassword
-rmHost <rm host name>
-dbType <db2/oracle>
-dbPort <database port number>
-dbSchema <database schema>
-pf <ORPHAN xml file>
-outputfile <output file for SQL statements>
-task <task>
```

where:

```
rmName          - Resource manager database name <db2>
                  or service name <oracle>
```

```

rmUserId      - Resource manager administrator id
rmPassword    - Resource manager administrator's password
rmHost        - Resource manager host name
dbType        - Type of Database (i.e. db2 or oracle)
dbPort        - Database port number (i.e. 50000 for db2,
               1521 for Oracle)
dbSchema      - Database schema (i.e. RMADMIN)
pf            - Name of Content Manager Validation Utility
               ORPHAN.xml file
output file   - Name of the SQL file
tasks        - The task to be executed
               Available tasks are:
                 1 - Find items reported
                 2 - Find items reported and build SQL script

```

Tip: An error message that is similar to the following message indicates that the environment is not set up correctly on the machine where you are running the validation utility recovery tool:

The java class is not found: com/ibm/mm/sdk/common/dkCollection

If you receive this message, complete the steps to set up the validation utility recovery tools.

3. Decide if you want to run the validation utility recovery tool against the error report data in the RMVALREPORT table or the error report data in a saved XML report (if applicable).

Option	Description
Run the recovery tool against the data in the RMVALREPORT table	<p>When you run the recovery tool against the data in the RMVALREPORT table, you must supply information about the database as values for the dbType, dbPort, and dbSchema parameters.</p> <p>Running the recovery tool against the data in the database means that you could be running the tool against older, cumulative report data or that expected report data could be missing if the RMVALREPORT data was manually cleared.</p>
Run the recovery tool against the data in a saved XML report	<p>If you configured the VALIDATION_XML_LOGPATH parameter to save validation utility report data as XML files, then when you run the recovery tool against the data in a saved XML report, you must supply the file name of the XML report file as a value for the pf parameter. The dbType, dbPort, and dbSchema parameters to supply information about the database are optional.</p> <p>Running the recovery tool against the data in the XML report file means that you are running the recovery tool against one set of error report data collected from a single scan by the validation utility.</p>

For the remainder of this procedure, the examples are shown with a choice to run the validation utility recovery tool against an XML file.

4. Run the ICMORPHANCleanup recovery tool in the mode to find orphan objects and build the SQL script, with the **task** parameter set to a value of 2. The following example shows how to run the command in the mode to find objects and build the SQL script.

```
java -cp ICMORPHANCleanup.jar;%CLASSPATH%
com.ibm.cm.rmtools.ICMORPHANCleanup
-rmName rmdb.example.com -rmUserid rmdadmin -rmPassword ce4win
-rmHost cmi375.example.com
-pf C:\temp\icmrmlsval20100907121957_ORPHAN.xml
-outputfile C:\temp\delete_ORPHAN.sql -task 2
```

5. Review the data in the SQL script against the data in the ORPHAN report, either in the RMVALREPORT table or the XML file.
6. Run the SQL script against the resource manager database to update the object status in the OBJ_STATUS column of the RMOBJECTS database table with a D flag, which marks the object for deletion. When the normal migrator process runs, the objects that are marked with the D flag are deleted from the resource manager storage volume.

Related tasks

“Setting up the validation utility recovery tools” on page 383

Repairing ITEMIDINVALID errors with the ICMITEMIDINVALIDCleanup recovery tool

You run the ICMITEMIDINVALIDCleanup validation utility recovery tool to fix ITEMIDINVALID errors reported by the validation utility.

Before you run the validation utility recovery tools, back up your library server and resource manager databases. There is no utility to reverse the changes that are made to the databases by the recovery tools.

If an object on the resource manager has an invalid item ID in the RMMIGRATIONTASKS table, then the validation utility flags this object with an ITEMIDINVALID error in the RMVALREPORT table. The ITEMIDINVALID error can occur during an upgrade from Version 8.3 to Version 8.4 when the migration task has pending transactions. The ICMITEMIDINVALIDCleanup validation utility recovery tool creates an SQL script. When the SQL script runs against the resource manager database, the script removes these invalid item IDs from the RMMIGRATIONTASKS table to repair this error condition.

Remember: The example commands in the following procedure are shown on multiple lines to improve readability. Enter the commands on a single line.

To run the ICMITEMIDINVALIDCleanup recovery tool:

1. Run the validation utility to generate the report data for the validation utility recovery tool.
2. Optional: Run the ICMITEMIDINVALIDCleanup validation utility recovery tool with no parameters to ensure that the API client environment is configured correctly and to view the help for all parameters. For example:

```
java -cp ICMITEMIDINVALIDCleanup.jar;%CLASSPATH%
com.ibm.cm.rmtools.ICMITEMIDINVALIDCleanup
```

This command returns the following usage information for the ICMITEMIDINVALIDCleanup recovery tool:

ERROR: Missing input parameters

Usage:

```
java -cp ICMITEMIDINVALIDCleanup.jar;%CLASSPATH%
com.ibm.cm.rmtools.ICMITEMIDINVALIDCleanup
  -rmName <db2name or oracle service name>
  -rmUserid
  -rmPassword
  -rmHost <rm host name>
  -dbType <db2/oracle>
  -dbPort <database port number>
  -dbSchema <database schema>
  -pf <ITEMIDINVALID xml file>
  -outputfile <output file for SQL statements>
  -task <task>
```

where:

```
rmName      - Resource manager database name <db2>
              or service name <oracle>
rmUserid    - Resource manager administrator id
rmPassword  - Resource manager administrator's password
rmHost      - Resource manager host name
dbType      - Type of Database (i.e. db2 or oracle)
dbPort      - Database port number
              (i.e. 50000 for db2, 1521 for Oracle)
dbSchema    - Database schema (i.e. RMADMIN)
pf          - Name of Content Manager Validation Utility
              ITEMIDINVALID.xml file
output file - Name of the SQL file
tasks       - The task to be executed
              Available tasks are:
                1 - Find items reported
                2 - Find items reported and build SQL script
```

Tip: An error message that is similar to the following message indicates that the environment is not set up correctly on the machine where you are running the validation utility recovery tool:

The java class is not found: com/ibm/mm/sdk/common/dkCollection

If you receive this message, complete the steps to set up the validation utility recovery tools.

- Decide if you want to run the validation utility recovery tool against the error report data in the RMVALREPORT table or the error report data in a saved XML report (if applicable).

Option	Description
Run the recovery tool against the data in the RMVALREPORT table	<p>When you run the recovery tool against the data in the RMVALREPORT table, you must supply information about the database as values for the dbType, dbPort, and dbSchema parameters.</p> <p>Running the recovery tool against the data in the database means that you could be running the tool against older, cumulative report data or that expected report data could be missing if the RMVALREPORT data was manually cleared.</p>

Option	Description
Run the recovery tool against the data in a saved XML report	<p>If you configured the VALIDATION_XML_LOGPATH parameter to save validation utility report data as XML files, then when you run the recovery tool against the data in a saved XML report, you must supply the file name of the XML report file as a value for the pf parameter. The dbType, dbPort, and dbSchema parameters to supply information about the database are optional.</p> <p>Running the recovery tool against the data in the XML report file means that you are running the recovery tool against one set of error report data collected from a single scan by the validation utility.</p>

For the remainder of this procedure, the examples are shown with a choice to run the validation utility recovery tool against an XML file.

- Run the ICMITEMIDINVALIDCleanup validation utility recovery tool in the mode to find the objects with invalid IDs and build the SQL script, with the **task** parameter set to a value of 2. The following example shows how to run the command in the mode to find objects and build the SQL script.

```
java -cp ICMITEMIDINVALIDCleanup.jar;%CLASSPATH%
com.ibm.cm.rmtools.ICMITEMIDINVALIDCleanup
-rmName rmdb.example.com -rmUserid rmdadmin -rmPassword ce4win
-rmHost cmi375.example.com
-pf C:\temp\icmrm\lval20100907121957_ITEMIDINVALID.xml
-outputfile C:\temp\delete_ITEMIDINVALID.sql -task 2
```

- Review the data in the SQL script against the data in the ITEMIDINVALID report, either in the RMVALREPORT table or the XML file.
- Run the SQL script against the resource manager database to remove the invalid item IDs from the RMMIGRATIONTASKS table.

Related tasks

“Setting up the validation utility recovery tools” on page 383

IBM Content Manager data validation utility for z/OS

The IBM Content Manager data validation utility for z/OS is a Java program that validates for inconsistency the data stored on a resource manager running on z/OS.

Use this utility if you suspect data inconsistency in your Content Manager for z/OS system.

The data validation utility can identify the following types of data inconsistency:

Orphan

An object is in the resource manager, but the library server does not have a reference to the object.

Not in resource manager

The library server has a reference to an object, but the object is not on the resource manager.

Size mismatch

The size of an object on the library server does not match the size of an object on the resource manager.

Collection mismatch

The collection referenced in the library server for the object does not match the collection that contains the object in the resource manager.

Date mismatch

The size and collection name match, but the creation or update dates for an object referenced on the library server do not match the dates of the object stored on the resource manager.

External object name discrepancy

A library server entry points to an incorrect or inaccessible resource manager entry.

Recommendations for when to run the data validation utility

You should run the data validation utility in the following situations:

- Run the utility after you migrate from an earlier version of IBM Content Manager for z/OS.
- Run the utility during periods of little or no server activity.

You can run the utility on a Microsoft Windows system, or under z/OS UNIX System Services. The utility connects to the Content Manager for z/OS server by a JDBC connection.

Related tasks

Installing and configuring the validation utility for z/OS

Validating data in Content Manager for z/OS

Related information

 DB2 Content Manager for z/OS data validation and cleanup utilities

Managing databases

The information related to the objects stored in the resource manager is maintained both in the library server and the resource manager. It is possible for data related to objects stored in the resource manager and library server to become unsynchronized. It is crucial to keep the data synchronized between the resource manager and library server. The resource manager provides utilities to help you synchronize the data. For more information about the resource manager utilities, see the information about resource manager utilities and services.

For related information pertaining to the z/OS environment, see the information about z/OS resource manager asynchronous processes

You also need to manage the objects that are stored in the database. The resource manager schedules when objects need to migrate and replicate. You can schedule migration and replication of objects when you configure resource managers for your system.

Optimizing server databases

A table can become fragmented after many updates, causing performance to deteriorate. Queries take longer because index entries in the library server and resource manager are no longer synchronized with the actual data in the database tables.

For an Oracle database, use the tools provided in Oracle to update the index and re-order as necessary.

You can synchronize the data in the index with the database tables by running the DB2 **REORGCHK** command.

The **REORGCHK** command gathers and compares both the index and the table statistics and recommends tables to reorganize. Most of the time, performance improves simply by running **REORGCHK**, but if it does not improve, you must reorganize the database tables.

When you reorganize tables, you remove empty spaces and arrange table data efficiently. Reorganizing tables takes longer than running **REORGCHK**. Do not reorganize tables when you expect a lot of server activity because performance will be slow. DB2 locks any data in a table that is currently being reorganized.

Consider the following factors to determine when to reorganize your table:

- The volume of insert, update, and delete activity.
- Running **REORGCHK** does not improve the performance of queries.

Though not advisable, you can reorganize a table at any time. If you update tables often, then you want to reorganize periodically. If you do not manage the DB2 database tables, you need to work with the DB2 administrator for access or to coordinate when to run **REORGCHK** and reorganize tables. See the DB2 Universal Database Information Center for usage information.

“Analyzing a DB2 database for optimization”

“z/OS resource manager exit programs” on page 396

Analyzing a DB2 database for optimization

If you manage the DB2 database, run periodic table updates by using the **REORGCHK** command.

To check and update database tables:

1. Open a DB2 command prompt and log in with an ID that has DB2 administrative (DBADM) authority.
2. When you run **REORGCHK**, store the results in a log file that contains the statistics you need to use to determine whether to reorganize a table. For example, if you want to update all of the tables, enter the following command:
`reorgchk update statistics on table all > out.txt`

where *out.txt* is the name of the log file.

3. Look at the Reorg column in your log file. DB2 Universal Database displays 1 to 3 asterisks (*) in the Reorg column when it detects a table to reorganize. The asterisks determine the urgency of reorganizing a table.

4. Note the schema name and table name (the first two columns). You use these two names to reorganize tables. For example, a schema name could be `icmadmin` or `sysibm` and a table name could be `icmstnlkeywords` or `sysindexes`.
5. For example, to reorganize the `sysindex` table, you might enter the following command:

```
reorg Table sysibm.sysindexes
```

6. Run **REORGCHK** again to see if you have any more tables to reorganize. Complete the previous steps to reorganize any other tables you want.
7. When you finish reorganizing database tables, rebind all packages by using the **db2rbind** command. You do not need to be connected to the database for this step. Enter the following command in the DB2 command window, where *icmnlsdb* is the name of the database and *report.txt* is the name of the log file that contains the results.

```
db2rbind icmnlsdb /l report.txt
```

Important: If you plan to update a schema that does not belong to you, you need a user ID and password. Also, the user ID and password must have DB2 administrative authority to complete this task.

8. Look at your log file or use the Control Center to see the results. To use the Control Center:
 - a. Start the DB2 Control Center:
 - On a UNIX system, enter `db2cc` in a DB2 command window.
 - On Windows, click **Start > Programs > IBM DB2 > Control Center**.
 - b. In the Control Center, go to the database against which you ran the **db2rbind** command.
 - c. In the database, go to **Application objects > Packages**.
 - d. Check the **Last bind date** and **Last bind time** columns. The date and time indicate when you last had DB2 rebind all the packages.

Related reference

 [db2rbind - Rebind all Packages Command](#)

 [REORGCHK Command](#)

z/OS resource manager exit programs

Exit program capabilities are provided in the IBM Content Manager resource manager for z/OS. Customers can execute exit programs before and after each type of order that the z/OS resource manager handles. Exit programs are given reserved names that describe their point of execution. More information, including a list of the reserved names, is provided in the "Installing and configuring IBM Content Manager" chapter of *Planning and Installing Your Content Management System for z/OS*.

Logging and tracing for IBM Content Manager

You can enable different levels of logging. You can also enable a trace on various components of the content management system.

You can enable the logging and tracing for the following components or services of Content Manager EE, Content Manager for z/OS, and IBM Information Integrator for Content:

- Installation
- Library server

- Resource manager
- System administration client
- Client for Windows
- eClient
- LDAP
- Java and C++ APIs
- HTTP server requests

You can configure logging and tracing for many of these components by using the common log control utility from the system administration client.

“Specifying log settings for IBM Content Manager components”

“Enabling tracing in IBM Content Manager” on page 406

“Enabling tracing in Content Manager for z/OS” on page 410

“Enabling the DSNTRACE resource manager DB2 trace facility” on page 414

“Enabling the HTTP Server trace facility” on page 414

“Event logging” on page 414

Specifying log settings for IBM Content Manager components

You can configure logging and tracing for many of the components by using the common log control utility from the system administration client.

To specify detailed logging instructions using the log control utility, complete the following steps:

1. In the system administration client, click **Tools > Log Configuration**. The Log Control Utility window opens.
2. On the General Logging Setting page, select the log level to apply to all components.
 - a. In the **Select Resource Manager** field, select the resource manager you want to work with.
 - b. In the **Choose log level to apply** field, select the log level.
 - c. Select each feature (for example, **System Administration Client**, **Library Server**, **Resource Manager**) that you want to use the selected level.
 - d. Click **Apply**.
 - e. If you want to set other features to a different level, repeat these steps.

Content Manager for z/OS: See “Enabling tracing in Content Manager for z/OS” on page 410 for specific instructions for Content Manager for z/OS.

3. Specify detailed log settings for any or all of the following components:
 - System Administration: Specify log settings for the system administration client and the LDAP user import utility.
 - Library Server: Specify log settings for the library server.
 - Resource Manager: Specify log settings for the resource managers.
 - APIs (Java): Specify log settings for Java APIs.
 - APIs (C++): Specify log settings for C++ APIs.
 - Beans: Specify log settings for JavaBeans.
4. Click **OK** to save changes and exit or **Apply** to save changes and continue working in the utility. You do not need to restart any component, but it can take a few minutes for changes to become active.

Log file descriptions

Log files have similar characteristics, such as time stamps, log IDs, and log controls.

For supported UNIX operating systems, IBM Content Manager uses a group user that associates specific access privileges to the update and control of log settings. The default group user name is `ibmcmgrp`. As a result, you can initially find the log configuration and log output in the home directory for that user (for example, `/home/ibmcmgrp`). This directory is called the working directory for IBM Content Manager. From that working directory, you can find the hierarchy of log configuration and log output files.

- Log configuration files are found in the `cmgmt` subdirectory (for example, `/home/ibmcmgrp/cmgmt`).
- Default log output files are found in the `log` subdirectory (for example, `/home/ibmcmgrp/log`).

For supported Windows operating systems, the IBM Content Manager working directory is equivalent to the path specified in the `IBMCMROOT` environment variable.

For the z/OS operating system, logs are output to `SYSPRINT`.

If client users experience errors, such as an error logging on to a content server or errors importing a document, you can use the `access.log` file to verify the resource manager Web address and to verify that the client request is getting through to the Web server.

The Web address that the client uses to access the resource manager can be configured from the system administration client. For information about how to configure resource manager Web settings, see the system administration client online help.

The IBM HTTP Server logs every client request in the `access.log` file.

The following list describes some examples of common log characteristics.

Common timestamp

All logs use Greenwich Mean Time (GMT) as the log time stamp standard for all logs.

Common log directory

By default, all log files are written to a common log directory. The log directory contains subdirectories for each system component. The installation program creates the log directory. The default location is `log` in the IBM Content Manager or IBM Information Integrator for Content working directory.

User-level tracing

User-level tracing allows you to start a trace for a specific user ID, such that debug tracing is automatically generated in the connectors of IBM Information Integrator for Content and the IBM Content Manager library server and resource manager only for that user ID. This capability avoids performance penalties for full component debugging for all users, and helps to collect only the information pertinent to that user. Use the system administration client to enable user-level tracing. User-level tracing requires the user application to log on again after the setting has been set to include the setting.

Dynamic log configuration

The changes that you make to the log configuration settings are effective within a few minutes.

Transaction correlation ID

This ID is generated by the APIs, and helps to identify specific user transactions throughout the system. This ID is especially useful in correlating logs between different components because the same ID per transaction, is logged in the logs. The transaction log correlation ID is written to the log files of the connectors of IBM Information Integrator for Content and the IBM Content Manager library server, resource manager, and the resource manager service or subprocess (for example, migrator) log files. A different transaction correlation ID is generated for each transaction scope to the library server.

Logging and tracing utility: system administration

You can provide additional logging control for the system administration client and the LDAP user import utility.

Important: The configuration information for the system administration client and the LDAP user import utility logging is saved on the system where the system administration client is installed, as are the log files. These settings apply only to this system.

1. In the Log Control Utility window, click **System Administration**. The System Administration Client and LDAP User Import Utility Logging page opens.
2. Specify the log file settings:
 - a. In the **Log File path** field, enter the path to the directory where you want to save the log files.
 - b. In the **Log File name** field, enter the name you want to give this log file. Do not remove the `{username}` token that appears at the beginning of this field. The username token identifies the operating system user logged in as the log file is written. If the token is removed, file permission errors might occur as the file is updated by multiple operating system users. The token results in the creation of unique log files from this component for each operating system user. You can change the second element of the file name, which identifies the component, and the file extension.
 - c. In the **Maximum log file size** field, enter a limit, in megabytes, for the log file. When the log file reaches this limit, a new file is created, up to the number specified in the **Maximum number of files** field.
 - d. In the **Maximum number of files** field, enter the number of log files you want to permit. When the number of log files reaches the maximum number you specify here, the system will start to overwrite older files instead of creating new ones.
3. Specify the logging level:
 - a. In the **Component to log** list, select which component you want to log.
 - b. Choose the logging level from the **Select logging level** list.
 - c. Click **Apply** to save the setting.
 - d. If you want to set the logging level for another component, repeat these steps.
4. Click **OK** to save changes and exit or **Apply** to save changes and continue working in the utility.

Logging and tracing utility: library server

You can provide additional logging control for the library server and optionally trace a specific user ID.

Important: The configuration information for the library server logging is saved on the system where the library server is installed, as are the log files.

1. In the Log Control Utility window, click **Library Server**. The Library Server Logging page opens.
2. Specify the log file settings:
 - a. In the **Log File path** field, enter the path to the directory where you want to save the log files.
 - b. In the **Log File name** field, enter the name you want to give this log file.
3. Choose the logging level for the library server from the **Select logging level** list.
4. Optional: In the **User name** field, specify the user ID of a single user you want to trace. The user ID must match the ID on the library server. By setting this option, the next time the specified user logs on, log output will be generated in the C++ or Java APIs, library server, and resource manager. Log output will be at a full trace level for this user. No other users will be logged.
5. Click **OK** to save changes and exit or **Apply** to save changes and continue working in the utility.

Logging and tracing utility: resource manager

You can provide additional logging control for the resource manager and optionally trace a specific user ID. If you have more than one resource manager, you must set the logging for each one separately.

The events for the resource manager services are logged in different log files, depending upon the type of event. The types of log files used for the resource manager can be divided into the logs that monitor the resource manager application during startup and the logs that monitor the resource manager events while the resource manager is running, as follows:

- The Java Virtual Machine (JVM) logs monitor whether the resource manager application starts correctly. These log files are the `SystemOut.log` and `System.err` files. By default, these files are located in the `${SERVER_LOG_ROOT}` path, where `SERVER_LOG_ROOT` is a WebSphere Application Server variable that is defined in the application server scope. The default for `SERVER_LOG_ROOT` is `${WAS_HOME}/profiles/${profileName}/logs/${serverName}`, where `WAS_HOME` is the installation directory of WebSphere Application Server, `profileName` is the name of the profile for the resource manager, and `serverName` is the name of the application server on which the application is deployed.

During resource manager initialization, the resource manager logs entries in the `SystemOut.log` file about the logging level (INFO, DEBUG, and so on) for the resource manager application, the location of the resource manager logging configuration file, the current contents of the logging configuration file, and the location of the resource manager application log file.

- The resource manager application log file monitors the resource manager application after it starts running. During resource manager initialization, a unique log file for that resource manager is generated by using the data in the logging configuration file, `icmrm_logging.xml`. The default name for this resource manager log file is `icmrm.logfile`. The default path for the file is `${SERVER_LOG_ROOT}/rm/rm_appname/icmrm.logfile`, or `${WAS_HOME}/profiles/`

`${profileName}/logs/${serverName}/rm/rm_appname/icmrm.logfile`, where `rm_appname` is the resource manager application name in WebSphere Application Server.

For resource managers in a clustered environment where multiple resource manager application servers are deployed in a single node, the process ID for each resource manager can be appended on the log file name, in the format `icmrm.logfile.process_ID`. This function is controlled by the Java system variable `icmrm.log4j.name.extension`. To change the value for `icmrm.log4j.name.extension` Java system variable, edit the JVM custom properties for the application server by using the administrative console in WebSphere Application Server.

Table 70. Values for the `icmrm.log4j.name.extension` Java system variable

Value of <code>icmrm.log4j.name.extension</code>	Definition
auto	Automatically detect whether the resource manager is in a clustered environment. If the resource manager is in a clustered environment, append the process ID to the log file name. The default value for <code>icmrm.log4j.name.extension</code> .
on	Append the process ID to the log file name.
off	Do not append the process ID to the log file name.

Important: The log file and the location of the log file are changed for Version 8.4.2. Your Version 8.3, Version 8.4, and Version 8.4.1 log configuration settings do not transfer to Version 8.4.2 during an upgrade. Beginning in Version 8.4.2, a new resource manager installation uses the default settings from the logging configuration file, `icmrm_logging.xml`, to set the location of the resource manager log file. The resource manager log files for Version 8.4.2 are set to a directory that is relative to where the resource manager is running.

If you upgrade IBM Content Manager and you want to keep the log configuration settings from your previous version, you must do one of the following actions:

- If you upgrade from any installation of Version 8.4 earlier than Version 8.4.2, including Version 8.4, Version 8.4.1 and fix packs for those versions, back up your current `icmrm_logging.xml` logging configuration file. After you upgrade to Version 8.4.2, you must use the `config_CM` configuration wizard utility to deploy the resource manager. Then restore the backup version of the `icmrm_logging.xml` file to the same location as the default logging configuration file.
- For all other upgrades, configure the log settings after upgrading by using the system administration client.

Important: Beginning in Version 8.4.2, file permissions for object files stored on the resource manager file system, including the log files, are changed. The default permission allows read permission on the files only to the user ID that created the file. Users who do not access the resource manager log files as root or as the administrator of the resource manager must know that the default file permission settings on the log files might prevent their access to these files.

To view the log files, use the log viewer in the WebSphere Application Server administrative console. To change the logging configuration settings for the

resource manager, use the IBM Content Manager system administration client. For example, you can change the logging level or have the system create a separate resource manager log file.

If you make changes to the resource manager log settings and want to go back to the default behavior, update the resource manager logging configuration from the IBM Content Manager system administration client and remove all values from the file path and file name.

The resource manager supports user-level tracing through the system administration client to the library server. You can also set the trace level to User for the resource manager subprocesses. If you want to enable user-level tracing by using the resource manager subprocesses, you must manually configure the subprocesses log configuration files.

The resource manager log includes log entries from all the resource manager services, such as the purger, migrator, stager, replicator, and so on. The logging level is the same for the resource manager and all its services. For example, if you set the resource manager log to the INFO level, then all services are set to the INFO log level. Log entries include the name of the service in each log entry. For example, the following log entry is for the replicator:

```
ICMRM:ENTRYEXIT 2009-05-21 22:13:42.027000 context:
[WorkManager.rm841fpa_RMWorkManager : 3]
- ==> deleteReplicationMetadataTask()
- deleteReplicationMetadataTask(RMMetadataManagerDB.java:231)
```

To change the logging configuration settings for the resource manager by using the system administration client:

1. In the Log Control Utility window, click **Resource Manager**. The Resource Manager Logging page opens.
2. Specify the log file settings:
 - a. In the **Log File path** field, enter the path to the directory where you want to save the log files.
 - b. In the **Log File name** field, enter the name you want to give this log file.
 - c. In the **Maximum log file size** field, enter a limit, in megabytes, for the log file. When the log file reaches this limit, a new file is created, up to the number specified in the **Maximum number of files** field.
 - d. In the **Maximum number of files** field, enter the number of log files you want to permit. When the number of log files reaches the maximum number you specify here, the system will start to overwrite older files instead of creating new ones.
3. Choose the resource manager you want to work with from the **Resource Manager** list.
4. Set logging levels for each resource manager component:
 - a. Choose the component to log from the **Component to log** list.
 - b. Choose the level you want to log at from the **Select logging level** list.

Tip: The following log levels in the system administration client correlate to the log levels that are enabled in the resource manager logging configuration file:

Table 71. Log levels in the system administration client and resource manager logging configuration file

Log levels in the system administration client	Log levels in the resource manager logging configuration file
error	error
warning	warn
informational	info
trace (entry and exit)	BEGINEND
trace (full)	DEBUG
performance	BEGINEND

- c. Click **Apply** to save the setting.
- d. If you want to set the logging level for another component, repeat these steps.

If you have multiple resource managers, remember to set logging levels for each one by repeating steps 3 and 4.

5. Click **Enable circular logging** to enable circular logging of the resource manager.
6. Click **OK** to save changes and exit or **Apply** to save changes and continue working in the utility.

Logging and tracing utility: Java APIs

You can provide additional logging control for Java APIs.

Important: The configuration information for the Java API logging is saved on the system where the system administration client is installed, as are the log files. These settings apply only to this system.

1. In the Log Control Utility window, click **APIs (Java)**. The APIs (Java) Logging page opens.
2. Specify the log file settings:
 - a. In the **Log File path** field, enter the path to the directory where you want to save the log files.
 - b. In the **Log File name** field, enter the name you want to give this log file. Do not remove the `${username}` token that appears at the beginning of this field. The username token identifies the operating system user logged in as the log file is written. If the token is removed, file permission errors might occur as the file is updated by multiple operating system users. The token results in the creation of unique log files from this component for each operating system user. You can change the second element of the file name, which identifies the component, and the file extension.
 - c. In the **Maximum log file size** field, enter a limit, in megabytes, for the log file. When the log file reaches this limit, a new file is created, up to the number specified in the **Maximum number of files** field.
 - d. In the **Maximum number of files** field, enter the number of log files you want to permit. When the number of log files reaches the maximum number you specify here, the system will start to overwrite older files instead of creating new ones.
3. Select the logging level from the **Select logging level** list.

4. Click **OK** to save changes and exit or **Apply** to save changes and continue working in the utility.

Logging and tracing utility: C++ APIs

You can provide additional logging control for C++ APIs.

Important: The configuration information for the C++ API logging is saved on the system where the system administration client is installed, as are the log files. These settings apply only to this system.

1. In the Log Control Utility window, click **APIs (C++)**. The APIs (C++) Logging page opens.
2. Specify the log file settings:
 - a. In the **Log File path** field, enter the path to the directory where you want to save the log files.
 - b. In the **Log File name** field, enter the name you want to give this log file. Do not remove the `${username}` token that appears at the beginning of this field. The username token identifies the operating system user logged in as the log file is written. If the token is removed, file permission errors might occur as the file is updated by multiple operating system users. The token results in the creation of unique log files from this component for each operating system user. You can change the second element of the file name, which identifies the component, and the file extension.
 - c. In the **Maximum log file size** field, enter a limit, in megabytes, for the log file. When the log file reaches this limit, a new file is created, up to the number specified in the **Maximum number of files** field.
 - d. In the **Maximum number of files** field, enter the number of log files you want to permit. When the number of log files reaches the maximum number you specify here, the system will start to overwrite older files instead of creating new ones.
3. Select the logging level from the **Select logging level** list.
4. Click **OK** to save changes and exit or **Apply** to save changes and continue working in the utility.

Logging and tracing utility: beans

You can provide additional logging control for Java beans.

Important: The configuration information for the beans logging is saved on the system where the system administration client is installed, as are the log files. These settings apply only to this system.

1. In the Log Control Utility window, click **Beans**. The Beans Logging page opens.
2. Specify the log file settings:
 - a. In the **Log File path** field, enter the path to the directory where you want to save the log files.
 - b. In the **Log File name** field, enter the name you want to give this log file. Do not remove the `${username}` token that appears at the beginning of this field. The username token identifies the operating system user logged in as the log file is written. If the token is removed, file permission errors might occur as the file is updated by multiple operating system users. The token results in the creation of unique log files from this component for each operating system user. You can change the second element of the file name, which identifies the component, and the file extension.

- c. In the **Maximum log file size** field, enter a limit, in megabytes, for the log file. When the log file reaches this limit, a new file is created, up to the number specified in the **Maximum number of files** field.
 - d. In the **Maximum number of files** field, enter the number of log files you want to permit. When the number of log files reaches the maximum number you specify here, the system will start to overwrite older files instead of creating new ones.
3. Select the logging level from the **Select logging level** list.
 4. Click **OK** to save changes and exit or **Apply** to save changes and continue working in the utility.

Configuring the resource manager log files

Each XML log configuration file contains default values that control the log file name, path, output type, size, and level of detail (typically set to the INFO level).

Each time that you use a resource manager service, such as the validator, the service generates a log file. If you receive an error when using a service, you can modify the default settings to gather more data and debug the problem.

Before you modify any configuration files, create a backup file.

Important: To modify a file, you must have write access to all of the directories where the configuration files are installed.

The different levels of logging include the following:

Fatal Logs only if the servlet terminates unexpectedly.

Action

Logs actions that the system administrator needs to take. This information does not describe errors, but conditions, such as “short on [disk] space.”

Error Logs information to indicate that a request was unable to be fulfilled or that an internal error occurred.

Warn Logs unexpected behavior.

Info Logs start or stop messages.

Request

Provides detailed information about the incoming request.

Response

Provides detailed information about the outgoing response.

Trace Logs general flow messages.

Debug

Provides detailed debugging information as well as information about all other priority levels.

Entryexit

Writes a trace line at the beginning of each function or method, and another trace line at the exit points of the functions or methods. This is often used by support to identify the location in the source code where a failure occurred.

The resource manager log files record action messages that contain steps about possible software problems that you can avoid. For example, an action message might inform you that the resource manager is filling its allotted volume of

messages. To avoid software difficulties, you can remove outdated information from the log files. The resource manager generates the action messages and appends the messages to the log files.

If you choose to send the logging information to a file that is different from the default configuration, you can follow your own naming conventions for the log file. You can also determine the expiration for these files. Expiration is determined by data size, instead of by date.

Important: The resource manager log manager continues to append log outputs to the existing log files. You can periodically delete obsolete data from the log files to help prevent them from becoming too large.

The resource manager uses Version 1.2.8 of log4j. For copyright and more information about the log4j configuration file, see the edition notices of the configuration files or go to <http://www.apache.org>.

Enabling tracing in IBM Content Manager

You can enable tracing using the system administration client.

To enable tracing and specify a tracing level:

“Enabling the library server trace facility”

Enabling the library server trace facility

By default, tracing is not enabled. However, you can enable tracing for the library server and specify the level of detail that you want in the trace. Note that enabling tracing has a negative impact on performance.

To enable tracing and specify a tracing level:

1. Log on to the system administration client as an administrator.
2. Expand your library server name and click **Library Server Parameters**.
3. Right-click **Configuration** and click **Explore**.
4. Right-click **Library Server Configuration** and click **Properties**.
5. In the Library Server Configuration window, click the **Log and Trace**.
6. Select the trace level and specify the trace file to write the trace. The initial value for the trace file name is set during the installation of IBM Content Manager library server. The default trace setting is No trace or 0.

When you select a positive trace level value, only the stored procedures that are being called are logged to the file. Specify a negative trace level to see the stored procedures and the parameter values that are being passed. You can define four trace, but not a negative value if you turn on library server tracing using the log control utility. Use the database command prompt method to define a negative trace level or to set a trace level higher than eight (8).

Important: The recommended Debug setting for the library server trace facility is -31. Selecting a trace level greater than -31 can result in slow performance for users because the system is sending a large amount of detail to the trace log file.

Table 72. Content Manager EE trace levels

Trace level	Description
0	No trace (default setting)
1	Basic trace, logs program flow

Table 72. Content Manager EE trace levels (continued)

Trace level	Description
2	Detail trace, logs program flow and data
4	Data trace
8	Performance trace
15	All of the above
16	Build/parse
31	All of the above
32	Memory management
63	All of the above

Table 73. Content Manager for z/OS trace levels

Trace level	Database setting	Information traced
No trace	0	
Basic trace	1	Entry and exit information to the IBM Content Manager stored procedures and lower-level library server functions.
Detailed	2	Basic trace information, plus information about the lower-level controls through the library server programming logic. This trace level provides information about how the program logic ran.
Data	4	Information about which input parameters were passed into the IBM Content Manager stored procedures, and the intermediate data as the stored procedures were running.
Performance	8	Information about how fast the IBM Content Manager stored procedures ran; the trace shows one line for each stored procedure and the elapsed time, in milliseconds, that the stored procedure took to run.
Basic and detailed	3	
Basic and data	5	
Basic and performance	9	
All options	15	Basic, detailed, data, and performance.
	16	Only build and parse, set using SQL.
	32	Memory management, set using SQL.
	63	All settings, build and parse, and memory management.

DB2 users

Use the DB2 Universal Database Control Center to view the contents of the table.

Oracle users

Use the Oracle Enterprise Manager to view the contents of the table.

Content Manager for z/OS users

If you specify an HFS file for the library server to write to, make sure the

user ID of ICMMLSWL has write permission to this file. To see the trace output, review the specified file. If you specify SYSPRINT, examine the contents of the file specified by the SYSPRINT DD of your workload manager job ICMMLSWL

“Library server trace facility”

“Defining trace values on DB2”

“Disabling the trace facility using DB2 commands”

“Defining trace values on Oracle” on page 409

“Disabling the trace facility by using Oracle commands” on page 409

“Finding the message for a SQL return code” on page 409

Library server trace facility: The system administration client is used to set the system trace level and location of the trace log. System trace information, by default, is written to ICMSEVER.LOG.

From a database perspective, the tracing is controlled by two parameters, TRACELEVEL and TRACEFILENAME, in the library server control table ICMSTSYSCONTROL.

Defining trace values on DB2:

To define the trace values on DB2:

1. Catalog the library server on the local system where you want to run the trace facility, or log on to the remote server where the library server is installed. Log on to the local or remote system with a user ID that has at least db2admin authority. For example, enter db2 connect to *dbname* user *user ID* using *password*.
2. Determine the current TRACELEVEL setting. The default setting is 0, which means that tracing is off. Enter db2 select tracelevel from icmstsyscontrol
3. Specify the trace level. See “Enabling the library server trace facility” on page 406 for trace level definitions. Enter db2 UPDATE icmadmin.ICMSTSysControl set TRACELEVEL = *tracelevel* where LIBRARYSERVERID = *x* and where *x* is the library server ID value. The value is defined during installation, and the typical value is 1.
4. Change the default trace log location by entering: UPDATE icmadmin.ICMSTSysControl set TraceFileName = *path/filename* where LIBRARYSERVERID = *x*.
5. Enter db2 connect reset.

The trace facility begins to collect trace information and write the information to the trace log file.

Disabling the trace facility using DB2 commands:

To disable the trace facility on DB2:

1. Catalog the library server database on your local system, or log on to the remote server where the database is installed. Be sure you log on to the local or remote system with a user ID that has at least db2admin authority.
2. At a DB2 prompt, enter the following command: db2 connect to *dbname* user *user ID* using *password*
3. Change the trace level to 0 to disable tracing. Enter the following command: db2 UPDATE icmadmin.ICMSTSysControl set TRACELEVEL = 0 where

LIBRARYSERVERID =*x* where *x* is the library server ID value. The ID value is defined during installation, and the typical value is 1.

4. Enter: db2 connect reset.

The trace facility stops collecting trace information.

Defining trace values on Oracle:

To define the trace values on Oracle, perform the following steps:

1. Log on to the remote server where the database is installed, or create an entry in the tnsnames.ora file on the local system where you want to run the trace facility, if the entry is not already created. Log on to the local or remote system with a user ID that has at least IBM Content Manager administration authority.
2. At the sqlplus command prompt, enter: connect *userID/password @ dbname*
3. Determine the current TRACELEVEL setting. The default setting is 0, which means that tracing is off. Enter the following command: select tracelevel from icmSTSysControl;
4. Specify the trace level. See “Enabling the library server trace facility” on page 406 for trace level definitions. Enter the following commands: db2 UPDATE icmadmin.ICMSTSysControl set TRACELEVEL = *x* LIBRARYSERVERID = *y*, where *x* is the new trace level, and *y* is the library server ID value. The ID value is defined during installation, and the typical value is 1.
5. Optional: Change the default trace log location by entering the following commands: UPDATE icmadmin.ICMSTSysControl set TraceFileName = *path/filename* where LIBRARYSERVERID = *y*.
6. Enter quit.

The trace facility begins to collect trace information and write the information to the trace log file.

Disabling the trace facility by using Oracle commands:

To disable the trace facility on Oracle on Solaris and AIX:

1. Log on to the remote server where the database is installed or create an entry in the tnsnames.ora file on the local system where you want to run the trace facility, if the entry is not already created. Log on to the local or remote system with a user ID that has at least IBM Content Manager administration authority.
2. At the sqlplus command prompt, enter: db2 connect to *dbname* user *user ID* using *password*.
3. Change the trace level to 0 to disable tracing. Enter: UPDATE icmadmin.ICMSTSysControl set TRACELEVEL =0 where LIBRARYSERVERID =*x*; *x* is the library server ID value. The ID value is defined during installation, and the typical value is 1.
4. Enter: disconnect.

The trace facility stops collecting trace information.

Finding the message for a SQL return code:

If an unexpected error occurs during an SQL operation in the library server, database SQL return codes are returned with the library return code ICM7015. SQL return codes are then documented in the library server log file with the SQL message.

To find a full explanation of a database SQL return code from the database interface:

Find the message:

Option	Description
DB2 users	<p>Enter db2cmd to open a DB2 command window, and enter from the command prompt <code>db2 ? sql0 nnn</code>, where <i>nnn</i> is the return code number after removing the negative sign.</p> <p>For example, to search for the DB2 SQL return code -818, enter: <code>C:\temp>db2 ? sql0818</code>.</p> <p>The command returns:</p> <p>SQL0818N A timestamp conflict occurred. Explanation: The timestamp generated by the precompiler at precompile time is not the same as the timestamp stored with the package at bind time.</p>
Oracle users	<p>See the Oracle error code documentation. On AIX and Solaris, enter <code>oerrfacility error</code>, where <i>facility</i> is the initial three-letter part of the error message and <i>error</i> is the number (after removing the negative sign).</p> <p>For example, to search for the Oracle return code ORA-7300, enter: <code>oerr ora 7300</code></p>

Restriction: On Windows servers, you must run the DB2 return code query from a DB2 command window.

As with the library server return codes, SQL return codes are generally used by system administrators, database administrators, and IBM Software Support representatives to diagnose problems. End users are not expected to act independently.

Enabling tracing in Content Manager for z/OS

In Content Manager for z/OS, the trace facility is provided as one of the installation programs for the library server and resource manager.

The library server and resource manager provide their own trace facility for system administrators and IBM Content Manager system programmers to perform problem determination. Users who enable these trace facilities must be aware that enabling tracing will have a negative impact on the performance of IBM Content Manager. In addition, the size of the trace file produced is very large. Users should plan ahead before enabling the trace facility.

“Enabling the library server trace facility for Content Manager for z/OS” on page 411

“Enabling the resource manager trace facility for Content Manager for z/OS” on page 412

Enabling the library server trace facility for Content Manager for z/OS

Enable the trace facility by logging on to the system administration client window and performing the following steps:

1. Expand your library server name and click **Library Server Parameters**.
2. Right-click **Configuration** and click **Explore**.
3. Right-click **Library Server Configuration** and click **Properties**.
4. In the Library Server Configuration window, click the **Log and Trace** tab.
5. Select the trace level that you want to enable and specify the trace file to write the trace. The initial value for the trace file name was loaded during the installation of the library server.

Table 74. Content Manager for z/OS trace levels

Trace level	Database setting	Information traced
No trace	0	
Basic trace	1	Entry and exit information to the IBM Content Manager stored procedures and lower-level library server functions.
Detailed	2	Basic trace information, plus information about the lower-level controls through the library server programming logic. This trace level provides information about how the program logic ran.
Data	4	Information about which input parameters were passed into the IBM Content Manager stored procedures, and the intermediate data as the stored procedures were running.
Performance	8	Information about how fast the IBM Content Manager stored procedures ran; the trace shows one line for each stored procedure and the elapsed time, in milliseconds, that the stored procedure took to run.
Basic and detailed	3	
Basic and data	5	
Basic and performance	9	
All options	15	Basic, detailed, data, and performance.
	16	Only build and parse, set using SQL.
	32	Memory management, set using SQL.
	63	All settings, build and parse, and memory management.

6. Click **OK** to exit the Library Server Configuration notebook and save the changes.

If you specify an HFS file for the library server to write to, make sure the user ID of ICMMLSWL has write permission to this file. To see the trace output, review the specified file.

If you specify SYSPRINT, examine the contents of the file specified by the SYSPRINT DD of your workload manager job ICMMLSWL.

Enabling the resource manager trace facility for Content Manager for z/OS

There are two methods of enabling the resource manager trace facility for Content Manager for z/OS: By using the log configuration utility in the system administration client, or by changing a value in the DB2 ICMRMCONTROL table.

“Enabling the resource manager trace facility for Content Manager for z/OS by using the log configuration utility”

“Enabling the resource manager trace facility by changing a value in the DB2 ICMRMCONTROL table” on page 413

Enabling the resource manager trace facility for Content Manager for z/OS by using the log configuration utility:

There are two methods of enabling the resource manager trace facility for Content Manager for z/OS. One method is to use the log configuration utility in the system administration client.

Ensure that the Resource Manager is active.

In the log configuration utility, you can set the resource manager trace level by selecting the logging level or by typing an integer value that adds two or more logging level values. This task describes both methods.

To set the resource manager trace level in the log configuration utility:

1. In the system administration client, click **Tools > Log Configuration**.
2. In the **General Log Settings** section of the Log Configuration Utility window, select a z/OS resource manager from the menu and click **Resource Manager**. A new window for z/OS resource manager log configuration opens.

Tip: If you select a non-z/OS resource manager, the new window does not contain the **z/OS Resource Manager logging** fields, and you are not able to specify the correct trace level. Be sure to select a z/OS resource manager.

3. Ensure that the resource manager for which you want to enable trace level logging is selected in the **z/OS Resource manager** menu. If it is not, then select the correct one.
4. Use one of the following methods to specify the trace level for the z/OS resource manager:

Method 1

In the **Logging level** menu, select one of the six predefined levels:

- 0 = Error
- 1 = Warning
- 2 = Informational
- 4 = Trace (entry/exit)
- 6 = Performance
- 15 = Trace (full)

Method 2

Add two or more of the following integer values and type the resulting value into the **Logging level** field:

- 0 = Error
- 1 = Warning
- 2 = Informational

- 4 = Trace (entry/exit)
- 8 = Debug

For example: 3 = Warning + Informational (1+2)

Important: Do not use values between 16 and 32767 without instruction from IBM Software Support.

5. Click **OK** to submit the request and close the window, or click **APPLY** to submit the request and keep the window open.

The resource manager trace facility for Content Manager for z/OS is enabled.

Viewing the trace level: To view the trace level, repeat steps 1 and 2, and select the z/OS resource manager that you want to view.

Enabling the resource manager trace facility by changing a value in the DB2 ICMRMCONTROL table:

There are two methods of enabling the resource manager trace facility for Content Manager for z/OS. One method is to enable the tracing facility by changing a value in a DB2 table.

When the HTTP server starts, and while it runs, it tracks the value of the TRACELEVEL attribute in the DB2 ICMRMCONTROL table.

Reset the TRACELEVEL in the ICMRMCONTROL DB2 table from its default of 0. Trace level values allow users to pick and choose which trace level they want in their logs by adding together the constants of the levels they want. For example, to log WARNING, INFO, and DEBUG use the value 11 (=1+2+8). To log all five levels use the value 15 (=1+2+4+8).

Table 75. Content Manager for z/OS resource manager trace levels

Trace level	Database setting	Information traced
ERROR	0	Logs information to indicate that a request was unable to be fulfilled or that an internal error occurred.
WARNING	1	Logs unexpected behavior.
INFO	2	Logs informational events. These events are not necessarily Errors or Warnings, but they may be of interest when performing problem determination.
ENTRYEXIT	4	Writes out a trace line at the beginning of each function or method, and another trace line at the exit points of the functions or methods. This is often used by support to identify the location in the source code where a failure occurred.
DEBUG	8	Provides detailed debugging information.

The output of the trace is written to the SYSPRINT DD of your HTTP server started task.

Enabling the DSNTRACE resource manager DB2 trace facility

DSNTRACE is a trace facility used to troubleshoot resource manager problems that are DB2 related. To configure it, you must add the following to your Web server procedure:

```
//STDERR DD SYSOUT=*,OUTPUT
//SYSOUT DD SYSOUT=*,OUTPUT
//CEEDUMP DD SYSOUT=*,OUTPUT
//DSNTRACE DD SYSOUT=*
```

Enabling the HTTP Server trace facility

In addition to using the IBM Content Manager resource manager trace facility, you can enable the HTTP Server trace facility. The parameters used by the HTTP Server are documented in the HTTP Server Procedure JCL.

To enable the trace facility, add -vv to the disposition parameter ICSPARM as shown:

```
ICSPARM='-p 80 -r /etc/icmmrmcf.conf -vv'
```

Browse the SYSOUT DD to find the trace output from the HTTP Server.

Event logging

IBM Content Manager can log system administration and item events for audit purposes. Logging is optional.

System administration events include actions performed by an administrator, either within the system administration client or in a custom application. These system administration events include events that define users, assign privileges, and assign access control lists to objects such as data objects, item types, or processes, events that allow others to access the database, and events that control where objects will reside and who will have access to them. These events are stored in the ICMSTSYSADMEVENTS table.

Important: Common Criteria users must enable logging of all events.

To enable or disable logging of system administration events, modify the library server configuration. Specifically, modify the log and trace information on the Log and Trace page of the library server configuration.

To view the contents of the ICMSTSYSADMEVENTS table, select one of the following methods according to your database type.

Table 76. Viewing methods for the ICMSTSYSADMEVENTS table

Database	Viewing method
DB2	Use the DB2 Control Center to view the contents of the table.
Oracle	Use the Oracle Enterprise Manager to view the contents of the table.

Item events are actions performed against specific objects within the resource manager, or the indexing information of the object within the library server. These events are stored in the ICMSTITEMEVENTS table. To enable or disable logging of item events, modify the item types you want to log. For each item type that you

want to enable logging for, you can specify which actions to log: create, retrieve, update, or delete. You can log any combination of the four actions.

The following information is logged:

- The event type (a code value), such as attempts to log on to the system and access objects.
- The user ID of the user who performed the action and if the action succeeded or failed.
- The date and time the event occurred.
- As many as four free-form text strings, which include information pertinent to the event.
- For item events only, the item ID of the object acted upon.

Important: For FIPS compliance, you must enable full logging of all events.

Because the data is stored in DB2 tables, you can issue various SQL select statements against the tables to filter events, search and sort the data, and create audit reports as needed. In addition, a list of event types (in text form, corresponding to the event codes in the event tables) is stored in the ICMSTNLSKEYWORDS table. By joining the event table with the keywords table, you can create an audit report which includes the event description instead of an event code. The text description of the event type can be used in SQL select statements and to search and sort data.

“Recognizing and maintaining full events tables”

“Removing entries from the events table”

“Searching and sorting the events table” on page 416

“ICM library server event table log” on page 418

Related tasks

“Logging item type events” on page 170

“Viewing or modifying log and trace information” on page 10

Recognizing and maintaining full events tables

The storage allocated to the two event tables, ICMSTSYSADMEVENTS and ICMSTITEMEVENTS, limits the maximum storable volume of event data. If one or both event tables reach their capacity, subsequent attempts to log events fail and the entire action is rolled back. Actions are rolled back until an administrator frees space by removing records from the event tables.

Use DB2 load and unload utilities to preserve all or part of the tables, copy them to other media, and later restore them if needed. See the DB2 Universal Database Information Center for information about loading data with DB2 Universal Database utilities.

Removing entries from the events table

When you use the IBM Content Manager system administration client, the library server records item and document routing related functions in the events table, ICMSTSYSADMEVENTS or ICMSTITEMEVENTS.

The events table grows with each logged event. To reduce the size of the events table, you can remove the expired and unused events from the table. The EventCode column in the events table indicates the classification of events as the following values:

1-200 System administration function event codes

200-900

Item, document routing, and resource management function event codes

1000+ Application event codes

You can delete events from the events table by performing either of these following tasks:

1. Log in to the server where the database exists.
2. Open a DB2 command prompt and connect to the library server database.
3. Optional: To delete an event for a system administration function from a library server, enter the following command on one line:

For example

```
delete from ICMSTSYSADMEVENTS where eventcode <=200 and  
Created < timestamp
```

where *timestamp* is a date and time in the format YYYY-MM-DD-
hh.mm.ss.xxxxxx, such as 2005-01-01-12.00.00.000000. For example:

```
delete from ICMSTSYSADMEVENTS where eventcode  
<=200 and Created < 2005-01-01-12.00.00.000000
```

4. Optional: To delete an event for an item function from a library server, enter the following command on one line:

```
delete from ICMSTITEMEVENTS where eventcode <=600 and  
Created < timestamp
```

where *timestamp* is a date and time in the format YYYY-MM-DD-
hh.mm.ss.xxxxxx, such as 2005-01-01-12.00.00.000000. For example:

```
delete from ICMSTSYSADMEVENTS where eventcode  
<=200 and Created < 2005-01-01-12.00.00.000000
```

5. Optional: To reclaim the file system space after you delete events, run the database reorganization utility on the library server database and then stop the database instance.

Searching and sorting the events table

To view specific information in the events tables, such as a type of event or events that happened during a date range, you can search and sort the tables.

Use SQL commands to manipulate the events tables, ICMSTSYSADMEVENTS and ICMSTITEMEVENTS. See IBM DB2 Universal Database: *Command Reference* (SC09-2951) or the DB2 Universal Database Information Center for command syntax.

1. Log in to the server where the database exists.
2. Open a DB2 command prompt and connect to the library server database.
3. At the DB2 command prompt, enter your query. The following example contains the basic syntax for a query:

```
select * from table_name T,  
          ICMSTNLSKEYWORDS K  
where K.KEYWORDNAME in ('keyword_name') and  
      K.KEYWORDCLASS = 16 and
```

```

K.KEYWORDCODE = T.EVENTCODE and
T.TIMESTAMP >= 'start_date' and
T.TIMESTAMP < 'end_date'
order by T.TIMESTAMP asc

```

The query is shown here on multiple lines to make it easier to read, but you should enter it on a single line.

Use the following variables in queries:

table_name

The name of the event table, either ICMSTSYSADMEVENTS or ICMSTITEMEVENTS.

T The correlation name of the table. Because the select statement joins the table you want to query with the keyword table ICMSTNLSKEYWORDS, you must indicate the table that each field belongs to. You do that by concatenating the correlation name with the table name using a period: *T.table_name*.

Attention: The examples that follow use these correlation names: S for the system administration event table ICMSTSYSADMEVENTS, I for the item event table ICMSTITEMEVENTS, and K for the keyword table ICMSTNLSKEYWORDS.

keyword_name

The name of the event you want to find. Use the event codes (without the number) listed in Table 79 on page 419. Always place the *keyword_name* inside parentheses and single quotation marks. If you want to specify multiple events, place each *keyword_name* inside single quotation marks, separate them with commas, and place them all within one set of parentheses. For example:

```
('event_1', 'event_2')
```

You can use the following command to query the keyword table ICMSTNLSKEYWORDS for a list of the types of events that are logged:

```
select KEYWORDNAME, KEYWORDCODE from ICMSTNLSKEYWORDS
where KEYWORDCLASS=16 order by KEYWORDNAME
```

start_date

The starting date and time is in the format YYYY-MM-DD-*hh.mm.ss.ttttt* where YYYY is the year, MM is the month, DD is the day, *hh* is the hour (using the 24-hour clock), *mm* is the minute, *ss* is the second, and *ttttt* represents milliseconds. For example, 2004-06-12-09.30.00.000000 means 9:30 AM on June 12, 2004. All elements are required, but you can use zeros for time elements (*hh*, *mm*, *ss*, and *ttttt*) that you do not want to consider. The date elements (YYYY, MM, and DD) must be non-zero integers.

end_date

The ending date and time, in the same format as the starting date.

The following commands are examples of typical queries on the event table. The queries are shown here on multiple lines to make them easier to read, but you should enter queries on a single line.

- List all add user, update user, and delete user commands between April 12, 2004 and April 17, 2004, in chronological order:

```
select * from ICMSTSYSADMEVENTS S,
            ICMSTNLSKEYWORDS K
where K.KEYWORDNAME in ('ADD USER', 'UPDATE USER', 'DELETE USER') and
      K.KEYWORDCLASS = 16 and
```

```

K.KEYWORDCODE = S.EVENTCODE and
S.TIMESTAMP >= '2004-04-12-00.00.00.000000' and
S.TIMESTAMP < '2004-04-17-00.00.00.000000'
order by S.TIMESTAMP asc

```

- List all update object actions performed by the user ID karinj on April 12, 2004, sorted by the item ID:

```

select * from ICMSTITEMEVENTS I,
          ICMSTNLSKEYWORDS K
where K.KEYWORDNAME in ('UPDATE OBJECT') and
      K.KEYWORDCLASS = 16 and
      K.KEYWORDCODE = I.EVENTCODE and
      I.USERID = 'karinj' and
      I.TIMESTAMP >= '2004-04-12-00.00.00.000000' and
      I.TIMESTAMP < '2004-04-13-00.00.00.000000'
order by I.ITEMID asc

```

- List all failed logon attempts on April 12, 2004, sorted by user ID:

```

select * from ICMSTSYSADMEVENTS S,
          ICMSTNLSKEYWORDS K
where K.KEYWORDNAME in ('ATTEMPT TO LOGON WITH INVALID USERID') and
      K.KEYWORDCLASS = 16 and
      K.KEYWORDCODE = S.EVENTCODE and
      S.TIMESTAMP >= '2004-04-12-00.00.00.000000' and
      S.TIMESTAMP < '2004-04-13-00.00.00.000000'
order by S.USERID asc

```

ICM library server event table log

Table 77 explains the information you see for event codes 1-208. These event codes are the system administration and logon event codes. You can disable the logging of events 1-88 and 500-522 by setting the SysAdminEventFlag value in ICMSTSYSCONTROL table to 0. To enable the logging, set the value to 1.

Table 77. System administration and logon event codes

Column name	Data type	Attribute
Event Code	Integer	NOT null
Created	Timestamp	NOT null
User ID	Char(32)	NOT null
EventData1	Varchar(254)	nullable
EventData2	Varchar(254)	nullable
EventData3	Varchar(254)	nullable
EventData4	Varchar(254)	nullable
EventData5	Varchar(254)	nullable

Table 78 on page 419 explains the data provided for item events. You can set the type of logging for this table by opening the ICMSTITEMTYPEDEFS table and defining the ItemEventFlag value. ItemEventFlag is used to tell the server to log an item's history, such as when it is created, updated, and so forth. The following value definitions perform the corresponding logging functions:

0 (Default): Do not log any events. Any value other than 0: Log document routing events.

The system uses bit-wise checking when determining logging for the following actions on an item:

Bit 0 Log create and reindex actions on an item.

Bit 1 Log retrieve actions on an item.

Bit 2 Log update actions on an item.

Bit 3 Log delete actions on an item.

Table 78. Item events table

Column name	Data type	Attribute
Event Code	Integer	NOT null
Created	Timestamp	NOT null
Item ID	Char(26)	NOT null
User ID	Char(32)	NOT null
EventData1	Varchar(254)	nullable
EventData2	Varchar(254)	nullable
EventData3	Varchar(254)	nullable
EventData4	Varchar(254)	nullable
EventData5	Varchar(254)	nullable

Table 79 describes the data you might see in the event log. Event codes 1 through 999 are reserved for library server functions. Event code 1000 and above are for user-defined functions. Event codes fall into the following categories:

- System administration functions: 1 through 88
- Logon functions: 201 through 209
- Resource manager object events: 210, 211, 531, 539, 607, 608, 609
- Item functions: 301 through 404
- Advanced workflow functions: 500 through 522
- Document routing events: 600 through 606, 616 through 618

Table 79. Library server event logging table

EventCode	EventData1	EventData2	EventData3	EventData4	EventData5
1 ADD USER	User ID	User Name	User Privilege Set	Grant Privilege Set	Default Item ACL
2 UPDATE USER	User ID	User Name	User Privilege Set	Grant Privilege Set	Default Item ACL
3 DELETE USER	User ID	N/A	N/A	N/A	N/A
4 ADD USER GROUP	Group User ID	Group Name	N/A	N/A	N/A
5 UPDATE USER GROUP	Group User ID	Group Name	N/A	N/A	N/A
6 DELETE USER GROUP	Group User ID	N/A	N/A	N/A	N/A
7 ADD ACL	ACL Code	ACL Name	Language Code	N/A	N/A
8 UPDATE ACL	ACL Code	ACL Name	Language Code	N/A	N/A
9 DELETE ACL	ACL Code	Language Code	N/A	N/A	N/A
11 INCREMENTAL UPDATE ACL	SP Name	Action	Privilege Set Code	Privilege Definition Code	N/A
12 ADD LANGUAGE	Language Code	Language Name	N/A	N/A	N/A

Table 79. Library server event logging table (continued)

EventCode	EventData1	EventData2	EventData3	EventData4	EventData5
13 UPDATE LANGUAGE	Language Code	Language Name	N/A	N/A	N/A
14 DELETE LANGUAGE	Language Code	N/A	N/A	N/A	N/A
15 ADD PRIVILEGE	SP Name	Action	Privilege Definition Code	Privilege Definition Name	Privilege Description
16 UPDATE PRIVILEGE	SP Name	Action	Privilege Definition Code	Privilege Definition Name	Privilege Description
17 DELETE PRIVILEGE	SP Name	Action	Privilege Definition Code	N/A	N/A
19 UPDATE SYS CONTROL PARM	ACL Binding Level	Library ACL Code	Public Access Enable	Default ACL Choice	SMS Choice
21 ADD ATTRIBUTE	Language Code	Attribute ID	Attribute Name	Attribute SQL Type	Attribute Length
22 UPDATE ATTRIBUTE	Language Code	Attribute ID	Attribute Name	Attribute SQL Type	Attribute Length
23 DELETE ATTRIBUTE	Language Code	Attribute ID	N/A	N/A	N/A
24 ADD ATTRIBUTE GROUP	Language Code	Attribute Group	Attribute Group Name	N/A	N/A
25 UPDATE ATTRIBUTE GROUP	Language Code	Attribute Group	Attribute Group Name	N/A	N/A
26 DELETE ATTRIBUTE GROUP	Language Code	Attribute Group	N/A	N/A	N/A
27 ADD COLLECTION NAME	RM Code	SMS Collection Code	User ID	Prefetch Indicator	SMS Collection Name
29 DELETE COLLECTION NAME	RM Code	SMS Collection Code	N/A	N/A	N/A
33 ADD COMPONENT	Component Type ID	Component Type Name	Component Type Description	Item Type ID	Parent Component Type ID
34 UPDATE COMPONENT	Component Type ID	Component Type Name	Component Type Description	User ID	N/A
35 DELETE COMPONENT	Component Type ID	Component Type Name	Component Type Description	N/A	N/A
36 BUILD COMPONENT TYPE	Schema Name	Component Type Name	Table Name	Item Type Name	Parent Component Type Name
37 ADD ITEM TYPE	Item Type ID	Item Type Name	Item Type Description	N/A	N/A
38 UPDATE ITEM TYPE	Item Type ID	Item Type Name	Item Type Description	N/A	N/A
39 DELETE ITEM TYPE	Item Type ID	Item Type Name	Item Type Description	N/A	N/A
40 GET ITEM TYPE	Number of Item Type ID	Detail	Number of Privilege Code	N/A	N/A

Table 79. Library server event logging table (continued)

EventCode	EventData1	EventData2	EventData3	EventData4	EventData5
41 ADD KEYWORD CLASS	Keyword Class	Keyword Code	Language Code	Keyword Name	Keyword Description
42 ADD KEYWORD CODE	Keyword Class	Keyword Code	Language Code	Keyword Name	Keyword Description
43 UPDATE KEYWORD CODE	Keyword Class	Keyword Code	Language Code	Keyword Name	Keyword Description
44 DELETE KEYWORD CODE	Keyword Class	Keyword Code	N/A	N/A	N/A
45 ADD LINK TYPE	Keyword Class	Keyword Code	Language Code	Keyword Name	Keyword Description
46 UPDATE LINK TYPE	Keyword Class	Keyword Code	Language Code	Keyword Name	Keyword Description
47 DELETE LINK TYPE	Keyword Class	Keyword Code	N/A	N/A	N/A
48 ADD PRIVILEGE SET	SP Name	Action	Privilege Set Code	Privilege Definition Code	N/A
49 UPDATE PRIVILEGE SET	SP Name	Action	Privilege Set Code	Privilege Set Name	Privilege Set Description
50 DELETE PRIVILEGE SET	SP Name	Action	Privilege Set Code	N/A	N/A
51 ADD COMPONENT VIEW	Component View ID	Component Type ID	Item Type ID	View Display Name	User ID
52 UPDATE COMPONENT VIEW	Component View ID	Component View Name	User ID	N/A	N/A
53 DELETE COMPONENT VIEW	Component View ID	Component View Name	Language Code	N/A	N/A
54 ADD ITEMTYPE VIEW	Item View ID	Item Type ID	ACL Code	Language Code	User ID
55 UPDATE ITEMTYPE VIEW	Item View ID	Item Type View Name	Language Code	N/A	N/A
56 DELETE ITEMTYPE VIEW	Item View ID	Language Code	N/A	N/A	N/A
57 ADD EVENT TYPE	Keyword Class	Keyword Code	Language Code	Keyword Name	Keyword Description
58 UPDATE EVENT TYPE	Keyword Class	Keyword Code	Language Code	Keyword Name	Keyword Description
59 DELETE EVENT TYPE	Keyword Class	Keyword Code	N/A	N/A	N/A
60 ADD SEMANTIC TYPE	Keyword Class	Keyword Code	Language Code	Keyword Name	Keyword Description
61 UPDATE SEMANTIC TYPE	Keyword Class	Keyword Code	Language Code	Keyword Name	Keyword Description
62 DELETE SEMANTIC TYPE	Keyword Class	Keyword Code	N/A	N/A	N/A
63 ADD XDO TYPE	XDO Class ID	Attribute Group ID	XDO Class Name	N/A	N/A

Table 79. Library server event logging table (continued)

EventCode	EventData1	EventData2	EventData3	EventData4	EventData5
64 UPDATE XDO TYPE	XDO Class ID	Attribute Group ID	XDO Class Name	N/A	N/A
65 DELETE XDO TYPE	XDO Class ID	N/A	N/A	N/A	N/A
66 ADD PRIVILEGE GROUP	Language Code	Privilege Group Code	Privilege Group Name	Privilege Group Description	Number of Privileges
67 UPDATE PRIVILEGE GROUP	Language Code	Privilege Group Code	Privilege Group Name	Privilege Group Description	N/A
68 DELETE PRIVILEGE GROUP	Language Code	Privilege Group Code	N/A	N/A	N/A
69 ADD SET ACL	ACL Code	User ID	User Kind	Privilege Set Code	N/A
70 UPDATE SET ACL	ACL Code	User ID	User Kind	Privilege Set Code	N/A
71 DELETE SET ACL	ACL Code	User ID	N/A	N/A	N/A
72 ADD COMPONENT ATTR	SP Name	Language Code	Component Type ID	Number of Attributes	N/A
73 ADD INDEX ON COMPONENT	SP Name	Action	Index Name	Component Type ID	Number of Attributes
74 DELETE INDEX ON COMPONENT	SP Name	Action	Index Name	N/A	N/A
75 ADD ITEM RELATION	Source Item Type ID	Target Item Type ID	N/A	N/A	N/A
76 UPDATE ITEM RELATION	Source Item Type ID	Target Item Type ID	N/A	N/A	N/A
77 DELETE ITEM RELATION	Source Item Type ID	Target Item Type ID	N/A	N/A	N/A
78 ADD ADMIN DOMAIN	Domain ID	Domain Name	Language Code	N/A	N/A
79 UPDATE ADMIN DOMAIN	Domain ID	Domain Name	Language Code	N/A	N/A
80 DELETE ADMIN DOMAIN	Domain ID	Language Code	N/A	N/A	N/A
81 ADD DOMAIN ACL	Domain ID	Number of ACL	N/A	N/A	N/A
82 DELETE DOMAIN ACL	Domain ID	Number of ACL	N/A	N/A	N/A
83 ADD DOMAIN PRIVILEGE SET	Domain ID	Number of Privilege Set	N/A	N/A	N/A
84 DELETE DOMAIN PRIVILEGE SET	Domain ID	Number of Privilege Set	N/A	N/A	N/A
85 CHANGE USER PASSWORD	User ID	Expiration Date	User Name	N/A	N/A
86 ADD AUTO LINK	Target Item Type Name	Source Item Type Name	N/A	N/A	N/A
87 UPDATE AUTO LINK	Target Item Type Name	Source Item Type Name	N/A	N/A	N/A

Table 79. Library server event logging table (continued)

EventCode	EventData1	EventData2	EventData3	EventData4	EventData5
88 DELETE AUTO LINK	Target Item Type Name	Source Item Type Name	N/A	N/A	N/A
201 LOGON	User ID	Event Time ddhhmmssmsms	Application	Password Flag	N/A
202 LOGOFF	User ID	N/A	N/A	N/A	N/A
203 LOGON INVALID USERID	User ID	Event Time	Application	N/A	N/A
204 LOGON INVALID PASSWORD	User ID	Event Time	Application	N/A	N/A
205 LOGON MAX USERS REACHED	User ID	Event Time	Application	N/A	N/A
206 LOG MAX USER ERROR REACHED	User ID	Event Time	Application	N/A	N/A
207 LOGON PASSWORD CHANGED	User ID	Event Time	Application	N/A	N/A
208 LOGON USER EXIT ERROR	User ID	Event Time	Application	N/A	N/A
209 USERCOUNT	User count	N/A	N/A	N/A	N/A
210 RMNOTAVAILABLE	"RM RMCODE ADDRESS port PORT NUMBER -- Changed to NOT AVAILABLE"	N/A	N/A	N/A	N/A
211 RMAVAILABLE	"RM RMCODE ADDRESS port PORT NUMBER -- Changed to AVAILABLE"	N/A	N/A	N/A	N/A
301 CREATE ITEM	Item Type Name	N/A	N/A	N/A	N/A
302 UPDATE ITEM	Old Version ID	New Version ID	Item Type Name	N/A	N/A
303 DELETE ITEM	Version ID	N/A	N/A	N/A	N/A
305 UPDATE OBJECT DATA	Version ID	Ext Object Name	Resource Length	N/A	N/A
306 REINDEX ITEM	Item Type Name	N/A	N/A	N/A	N/A
401 GET ITEM	Component ID	Component View Name	Item Type View Name	N/A	N/A
500 ADD WORKFLOW ACTION	Action Code	Action Name	Language Code	Predefine Action	N/A
501 UPDATE WORKFLOW ACTION	Action Code	Action Name	Language Code	Predefine Action	N/A
502 DELETE WORKFLOW ACTION	Action Code	Action Name	Language Code	N/A	N/A

Table 79. Library server event logging table (continued)

EventCode	EventData1	EventData2	EventData3	EventData4	EventData5
503 ADD WORKFLOW ACTIONLIST	SP Name	Action	Action List	N/A	N/A
504 UPDATE WORKFLOW ACTIONLIST	SP Name	Action	Action List	Action List Name	Action List Description
505 DELETE WORKFLOW ACTIONLIST	SP Name	Action	Action List	N/A	N/A
506 ADD WORKFLOW DIAGRAM	SP Name	Action	Diagram ID	Diagram Name	Diagram Description
507 UPDATE WORKFLOW DIAGRAM	SP Name	Action	Diagram ID	Diagram Name	Diagram Description
508 DELETE WORKFLOW DIAGRAM	SP Name	Action	Diagram ID	N/A	N/A
509 CHECKIN DIAGRAM	SP Name	Action	Diagram ID	Diagram Name	Diagram Description
510 CHECKOUT DIAGRAM	SP Name	Action	Diagram ID	Diagram Name	Diagram Description
511 ADD WORKLIST	Work List Code	ACL Code	Language Code	Work List Name	Work List Description
512 UPDATE WORKLIST	Work List Code	ACL Code	Language Code	Work List Name	Work List Description
513 DELETE WORKLIST	Work List Code	N/A	N/A	N/A	N/A
514 ADD COLLECTION POINT	SP Name	Action	Process ID	Collection Activity ID	WF Starter ID
515 UPDATE COLLECTION POINT	SP Name	Action	Process ID	Collection Activity ID	WF Starter ID
516 DELETE COLLECTION POINT	SP Name	Action	Process ID	N/A	N/A
517 ADD WORKFLOW EVENT	Activity ID	Process ID	WF Starter ID	N/A	N/A
518 UPDATE WORKFLOW EVENT	Activity ID	Process ID	WF Starter	N/A	N/A
519 DELETE WORKFLOW EVENT	Activity ID	N/A	N/A	N/A	N/A
520 ADD DIAGRAMPROMPT	SP Name	Action	Diagram ID	Number of Prompts	N/A
521 UPDATE DIAGRAMPROMPT	SP Name	Action	Diagram ID	Number of Prompts	N/A
522 DELETE DIAGRAMPROMPT	SP Name	Action	Diagram ID	Number of Prompts	N/A

Table 79. Library server event logging table (continued)

EventCode	EventData1	EventData2	EventData3	EventData4	EventData5
531 RETRIEVE OBJECT	Part version ID	Document item ID	Document version ID	resource manager name	N/A
539 SETUP RM FLAG	RM Name	N/A	N/A	N/A	N/A
600 DR START PROCESS	Process Name	Work Node Name	N/A	Work Package Component ID	N/A
601 DR ROUTE ITEM	Process Name	Work Node Name	Next Work Node Name	Work Package Component ID	N/A
602 DR END PROCESS	Process Name	Work Node Name	N/A	Work Package Component ID	Normal process completion or Abnormal process completion
605 DR OVERLOAD	Process Name	Work Node Name	Number of Work Packages Currently in Work Node	Work Package Component ID	N/A
606 DR WORKNODE PASSTHROUGH	Process Name	Work Node Name	N/A	N/A	N/A
607 ADD REPLICA RULES	Source RM Name	Target SMS Collection Code	Number of Replica Rules	N/A	N/A
608 DELETE REPLICA RULES	Source RM Name	Target SMS Collection Code	Number of Replica Rules	N/A	N/A
609 UPDATE REPLICA RULES	Source RM Name	Target SMS Collection Code	Number of Replica Rules	N/A	N/A
616 DR SUSPEND WORKPACKAGE	Process name	Work node name	Expiration time set for this work package, if applicable	Work Package Component ID	N/A
617 DR RESUME WORKPACKAGE	Process name	Work node name	N/A	Work Package Component ID	N/A
618 DR AUTOMATIC RESUME WORKPACKAGE	Process name	Work node name	N/A	Work Package Component ID	N/A

Managing user access

You allow users access to the IBM Content Manager system by creating user IDs, passwords, and privilege sets.

To define user IDs with the proper access, you need to do the following steps:

- Find the appropriate privileges to create privilege sets.
- Assign privilege sets to the users to allow them to do what their jobs require.
- Create access control lists (ACLs) to restrict access to certain objects.
- Assign user IDs to ACLs to specify their access to objects.

After defining individual user IDs, you might also want to organize them by grouping them with other user IDs with similar access needs or similar job requirements. User groups allow you to conveniently organize your user IDs so that you can find specific user IDs easily.

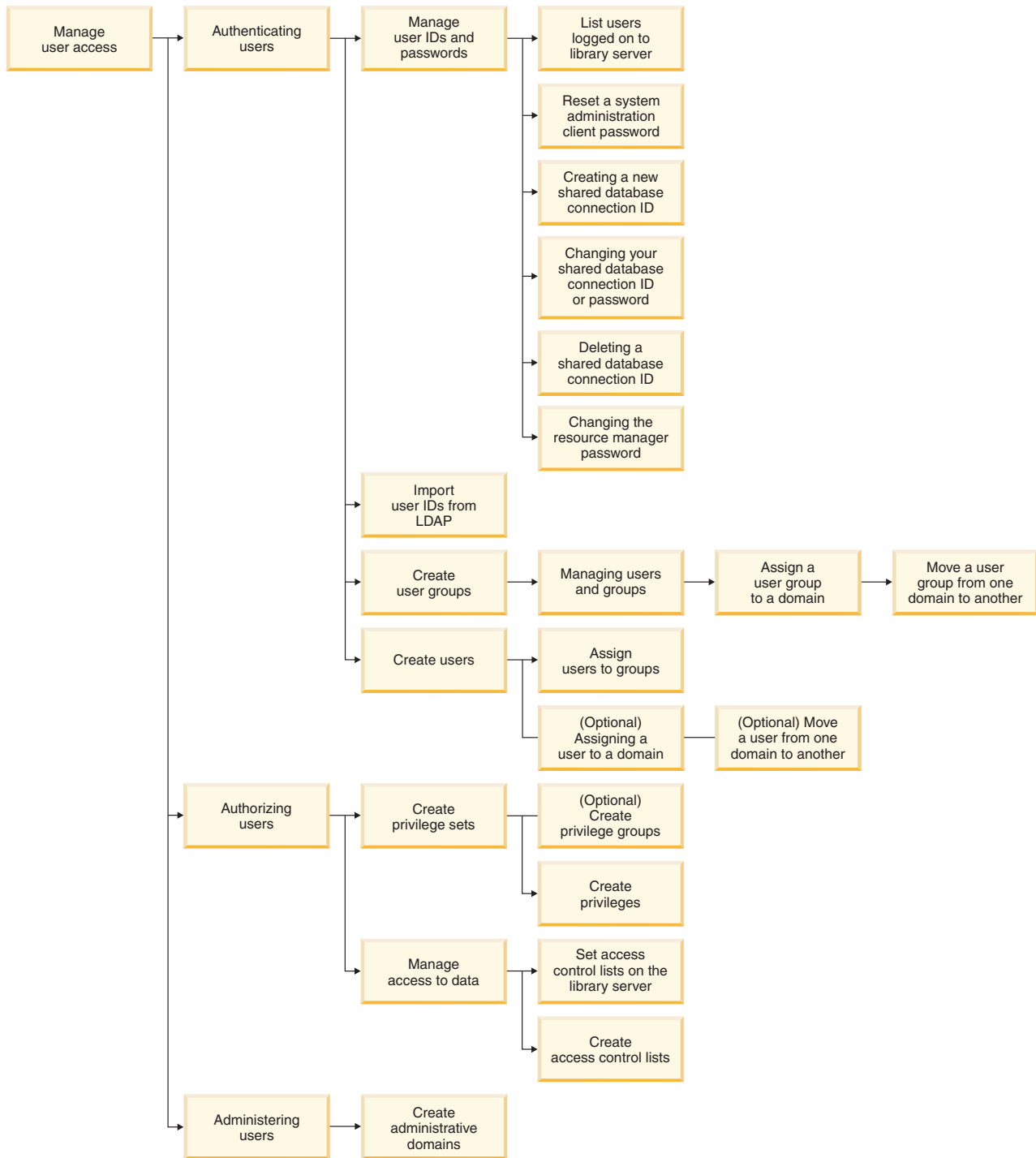


Figure 26. Common tasks related to managing user access

Authenticating users

Authenticating users includes managing, creating, and importing user IDs and passwords.

Managing user IDs and passwords

Managing user IDs and passwords includes changing, deleting, and listing user IDs and resetting passwords.

Administration authority

When logging on to the system administration client, you have two levels of authentication: one at the database level and another at the product level. Administrators have two classifications when you enable the administrative domains feature: superadministrators and subadministrators. In general, only superadministrators have unrestricted access to the system administration client.

“DB2 administration authority”

“Oracle administration authority”

DB2 administration authority:

For DB2, superadministrators must have the DBADM authority.

That is, full administrative privileges to DB2 are required. This user ID has to be defined in the operating system with the DB2 administrator privilege. The password for this operating system ID is used to connect to DB2 and to log on to the library server. The password defined for the library server is not used. IBM Content Manager does not store the password for the administrator. This user ID is defined in the library server with full IBM Content Manager administration privileges (AllPrivs) to perform all administration activities.

Important: If you upgrade your database to DB2 Version 9.7, then you must explicitly grant the DBADM database administration authority to superadministrators. If an existing superadministrator was granted the DBADM authority in an earlier version of DB2 through a group that contains that user ID, then that user ID does not retain the DBADM authority when you upgrade to DB2 Version 9.7. To ensure that all IBM Content Manager superadministrators retain the authority to work with both users and data modeling objects such as item types, you must explicitly grant the DBADM authority to each superadministrator user ID.

Tip: If you want to create a new IBM Content Manager administrator, use the system administration client to create an IBM Content Manager user with the same name as the operating system user and assign the appropriate system administration privilege set.

Subadministrators do not require DB2 privileges. Subadministrators manage only certain sections of the library server. Therefore, subadministrators log on to the system administration client in one of two ways:

- If the user ID is an operating system user ID, then the password in the operating system is used to connect to DB2 and to log on to the library server.
- If the user ID is not an operating system user ID, then IBM Content Manager will use a shared connection ID then will use a shared connection ID, such as ICMCONCT, to connect to DB2. The user ID and password that are provided in the Logon window are used to log on to the library server.

Oracle administration authority:

For Oracle, superadministrators must have the minimum database privileges to use IBM Content Manager.

To create a new superadministrator, use the following script:

`IBMCMROOT/config/icmlsorausr.sql`

This script creates the database user and grants the user the minimum privileges to use IBM Content Manager. The user ID can be used to directly connect to Oracle and to log on to the library server. The library server does not store the password for this user ID.

Tip: If you want to create a new IBM Content Manager administrator, run the script. Then, use the system administration client to create an IBM Content Manager user with the same name as the database user and assign the appropriate system administration privilege set.

Subadministrators are not required to be database users. Subadministrators manage only certain sections of the library server. Therefore, subadministrators log on to the system administration client in one of two ways:

- If the user ID is also a database user ID, then the user ID can be used to connect to Oracle and to log on to the library server.
- If the user ID is not a database user ID, then IBM Content Manager will use a shared database connection ID, such as ICMCONCT, to connect to Oracle. The user ID and password that are provided in the Logon window are used to log on to the library server.

Connecting to DB2 or Oracle by using a shared connection ID

Users who are defined only as IBM Content Manager users can connect to DB2 or Oracle by using a shared, encrypted user ID and password that is defined during installation.

With the shared database connection ID, you can connect to the database where your server is located. Then the database, or another server such as an LDAP directory server, authenticates the user ID and password.

Before you can create the shared database connection ID, you must create an operating system user or database user, depending on your database type.

To create an operating system user or database user:

Database	Task
DB2	Create a new operating system user ID and assign the minimum privileges necessary for use with IBM Content Manager.
Oracle	Run the <code>IBMCMROOT/config/icmlsorausr.sql</code> script to create a new database user ID and assign the minimum privileges necessary for use with IBM Content Manager.

After you create the operating system user or database user, you must create a new shared database connection ID in IBM Content Manager and update it in the INI file by following the steps in the next two sections.

1. "Creating a new shared database connection ID for IBM Content Manager"
2. "Changing the shared database connection ID and password" on page 431

Creating a new shared database connection ID for IBM Content Manager:

IBM Content Manager users can connect to the database server by using a shared database connection ID.

The default shared database connection ID is ICMCONCT.

To create a new shared database connection ID:

1. In the system administration client, click **Tools > Manage Database Connection ID > New Database Connection ID**.

2. In the **User ID** field, type the shared database connection user ID.

3. Select **Password is required for all users logging on to CM** if you want the user to enter a password when they log on to the system. When the checkbox for the UserDBConnect privilege set is selected, then the UserDBConnect privilege set is assigned to the user ID. If the checkbox is not selected, then the UserDBTrustedConnect privilege set is assigned to the user ID.

You can assign the UserDBConnect privilege set for IBM Content Manager users who do not have individual DB2 or Oracle user IDs and passwords. IBM Content Manager uses the shared IBM Content Manager user ID to connect IBM Content Manager users to DB2 or Oracle, without requiring them to have their own DB2 or Oracle user ID and password.

Alternately, you can use the UserDBTrustedConnect privilege set for users who authenticate through an LDAP server or other authentication software when those users log in to IBM Content Manager. After the IBM Content Manager user ID is authenticated, the IBM Content Manager user can log on to IBM Content Manager without a password.

4. Click **OK** to save the changes.

Important: Stored procedures for logon will check in the ICMSTUsers table for the shared database connection ID. If the ID is not defined in the table, an error will occur when attempting to log on to the database.

Before you can use the shared database connection ID to connect to IBM Content Manager, you must change the ID to update it in the INI file.

Changing the shared database connection ID and password:

Before you connect to IBM Content Manager by using the shared database connection ID for the first time, you must change the shared database connection ID to update it in the INI file. You might want to change the shared database connection ID and password periodically for security reasons.

To change your shared database connection ID and password:

1. In the IBM Content Manager system administration client, click **Tools > Manage Database Connection ID > Change Shared Database Connection ID**.
2. In the **User ID** field, enter the shared database connection ID.
3. In the **Password** field, enter the password. The password is case-sensitive.

Database	Password
DB2	Use the password for the operating system user ID.
Oracle	Use the password for the database user ID.

4. In the **Confirm Password** field, retype the password.

5. Select **Password is required for all users logging on to CM** if you want users to enter a password when they log on to the system. When the check box for the UserDBConnect privilege set is selected, then the UserDBConnect privilege set is assigned to the user ID. If the checkbox is not selected, then the UserDBTrustedConnect privilege set is assigned to the user ID.

You can assign the UserDBConnect privilege set for IBM Content Manager users who do not have individual DB2 or Oracle user IDs and passwords. IBM Content Manager uses the shared IBM Content Manager user ID to connect IBM Content Manager users to DB2 or Oracle without requiring them to have their own DB2 or Oracle user ID and password.

Alternately, you can use the UserDBTrustedConnect privilege set for users who authenticate through an LDAP server or other authentication software when those users log in to IBM Content Manager. After the IBM Content Manager user ID is authenticated, the IBM Content Manager user can log on to IBM Content Manager without a password.

6. Click **OK** to save the changes.

Important: Stored procedures for logon will check in the ICMSTUsers table for the shared database connection ID. If the ID is not defined in the table, an error will occur when you log on to the database.

User ID and password rules

If you want a user ID that you define in the system administration client to also be used for DB2 or Oracle database authentication, then the user ID must follow the DB2 or Oracle naming rules.

The DB2 or Oracle naming rules apply for user IDs that you want to use for either superadministrators or connect user IDs.

1. "DB2 ID and password rules"
2. "Oracle ID and password rules" on page 433

DB2 ID and password rules:

When defining a user ID in the system administration client, follow the DB2 naming rules if you want also want to use the ID for DB2 database authentication.

You cannot use the following words for a user ID:

- USERS
- ADMINS
- GUESTS
- PUBLIC
- LOCAL
- Any SQL reserved word listed in the SQL Reference

You cannot begin a user ID with the following characters:

- SQL
- SYS
- IBM

You can use the following characters for a user ID:

- A through Z
- 0 through 9

- #
- \$

IBM Content Manager supports the following password characters across all client applications:

- All English letters, both uppercase and lowercase
- Numeric digits 0 through 9
- The space character
- The following characters: ! # \$ % & ' () * + , - . / : ; < = > ? @ ^ _

Tip: By default, the library server does not limit the characters that users can enter for passwords. Even characters that are not in the previous list can be entered, potentially creating passwords that are incompatible between different client applications. If you want to ensure that passwords are compatible across all clients during password creation, use the ICMValidatePassword user exit.

Restrictions:

- Some operating systems allow case-sensitive user IDs and passwords. Check your operating system documentation to see if it allows for case-sensitivity.
- The maximum length of the user ID is 30 characters, unless the operating system imposes additional restrictions. Passwords are not limited in length unless the operating system imposes additional restrictions.
 - **DB2 on UNIX:** User IDs are limited to 8 characters.
 - **z/OS:** User IDs and passwords are limited to 8 characters.
- If you grant specific database access authorities to a user ID, a group can not exist that has the same name as that user ID.

Oracle ID and password rules:

When you are defining a user ID in the system administration client, follow the Oracle naming rules if you want also want to use the ID for Oracle database authentication.

IBM Content Manager supports the following password characters across all client applications:

- All English letters, both uppercase and lowercase
- Numeric digits 0 through 9
- The space character
- The following characters: ! # \$ % & ' () * + , - . / : ; < = > ? @ ^ _

Tip: By default, the library server does not limit the characters that users can enter for passwords. Even characters that are not in the previous list can be entered, potentially creating passwords that are incompatible between different client applications. If you want to ensure that passwords are compatible across all clients during password creation, use the ICMValidatePassword user exit.

Related information

 Oracle naming rules

Changing the resource manager database access passwords

To change the resource manager database access passwords, you must change the password for the database connection and the datasource connection information so that the resource manager can identify the new password.

To change the resource manager database access passwords, you must first complete the following tasks:

- DB2 users: Change the operating system password for the database connection by completing the following steps:
 1. Depending on your operating system, navigate to the Users and Passwords utility.
 2. Identify your resource manager administrator ID.
 3. Change your password.
- Oracle users: Change the database password for your resource manager administrator ID.

To change the datasource connection password, complete the following steps:

1. Connect to the WebSphere Application Server administration console.
2. Expand the WebSphere Application Server resources submenu, then expand the JDBC submenu and click **Data sources**.
3. Select the corresponding datasource for your resource manager. For example, RMAPNAME_database.
4. Click **JAAS - J2C authentication data** and update the authentication information with your new password.

After you change the Oracle database password or operating system password that is used to connect to the DB2 database, you must restart the resource manager database and the resource manager application.

Deleting the database connection ID

When a shared database connection ID is modified using the **Change Shared Database Connection ID and Password** window, the new user ID is updated in the INI file and added to the library server, but the old one is not deleted because it could still be in use by other library servers.

To delete a shared database connection ID that is not being used:

1. In the System Administration Client window, click **Tools > Manage Database Connection ID > Delete Database Connection ID** to open the Delete Database Connection ID window.
2. In the **User ID** field, select the shared database connection ID that you want to delete.
3. Click **OK** to save the changes.

Listing users currently logged on to the library server

In IBM Content Manager, you can obtain a list of the users who are logged on to a library server. The list includes the user ID of each logged-on user.

You can access the List Users window to estimate the number of users who are currently logged on to the system. You can use this functionality, for example, to detect any large increases or decreases in active users over time.

Restriction: In an IBM Content Manager system where multiple logons occur using the same user ID or where an application terminates without logging off users, the count is not accurate. IBM Content Manager marks a user as logged off when a log off is executed, regardless of how many instances of the same user IDs are logged in.

To list the logged-on users:

1. Click **Tools > List Users** to open the List Users window.
2. Click **OK** to close the window.

Managing users with LDAP

LDAP (Lightweight Directory Access Protocol) supports the management of user IDs and passwords at an enterprise level instead of management of this data on individual systems. You can use LDAP with Content Manager EE.

LDAP is an open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

LDAP manages groups, user IDs, and passwords on an enterprise level, rather than on a system-by-system basis. Most likely, you already have a directory of user IDs created for your business. Many of these user IDs share access privileges to information. Instead of creating or importing one user ID at a time, you can import user IDs from the existing directory and assign access privileges to several user IDs at one time. Content Manager EE uses LDAP by importing users and groups to the library server while still using LDAP to authenticate the users. The use of LDAP with Content Manager EE can reduce the user maintenance workload for the Content Manager EE administrator, particularly in a content management system with many users.

During the process to integrate LDAP with Content Manager EE, user name information is imported from the LDAP directory to the library server where it is stored as an entity reference. The password is not imported and is still stored in the LDAP server. After LDAP integration is complete, a user can log on to a Content Manager EE client and the user credentials are authenticated with the LDAP server.

Content Manager EE and IBM Information Integrator for Content use these LDAP technologies:

- IBM Tivoli Directory Server
- Lotus Domino® Address Book
- Microsoft Active Directory
- Novell eDirectory
- Sun Java Directory Server

You can complete LDAP integration either during installation or after installation. However, the integration steps include tasks that must be performed for the system administration client, library server, and resource manager. In addition, the integration might involve people with expertise in different areas of the entire content management system, including the Content Manager EE installer, the Content Manager EE system administrator, the LDAP administrator, and others. For these reasons, integrating LDAP after Content Manager EE installation is recommended.

During LDAP integration, you import LDAP users. After the import, you can use the system administration client to modify user attributes according to the requirements of your content management system. You can import user IDs by using an automatic or manual method.

The automatic method of importing users is by using the LDAP user import utility. The utility is a convenient way to import many LDAP groups and users into a Content Manager EE or IBM Information Integrator for Content database for the first time. In addition, the LDAP user import utility contains capability to schedule periodic updates of user ID information from the LDAP directory to the library server. This update helps to ensure that users added to or deleted from the LDAP directory are also added to or deleted from the system database.

The manual method of importing users from LDAP is available from the system administration client Content Manager EE. This method is the most convenient way to import an individual user or a few users after the initial setup of your LDAP users with the automatic method. The manual method is also used to test your connection to LDAP.

When LDAP is integrated with Content Manager EE, the user password resides on the LDAP server. When a user logs on to Content Manager EE, the user ID and password are authenticated and the specific privileges of the user ID are checked by the user profile in the corresponding database. During logon, the library server automatically connects to the LDAP server to authenticate the user. If for any reason the LDAP server is not able to verify the password of the user, the authentication fails.

For information about planning for LDAP, see *Planning and Installing Your Content Management System*.

“Integrating LDAP with Content Manager EE”

“Manually importing user IDs from an LDAP directory server” on page 456

Integrating LDAP with Content Manager EE

To integrate LDAP with your content management system, you must set up Content Manager EE to connect with LDAP, import the LDAP users to the library server, and set up LDAP user authentication.

The end-to-end process to integrate LDAP with your Content Manager EE system includes the following high-level groups of tasks:

- Set up the LDAP configuration in the content management system.
 - Generate the properties file to contain LDAP connection information.
 - Create a test user to test the LDAP connection with the LDAP user search function in the system administration client.
 - Add the properties file to the library server and resource manager as required by your configuration.
- Import LDAP users into the library server. To use the most efficient method, set up the LDAP user import utility to import the users and synchronize user data after the initial import action.
- Set up LDAP user authentication.
 - Install the Content Manager EE LDAP user exit that sends LDAP user information to the LDAP server for authentication.
 - Install the IBM Tivoli Directory Server client on the library server machine. This client contains the libraries that the LDAP user exit requires during user authentication.
 - Optionally, set up Secure Sockets Layer (SSL) for LDAP authentication.
 - Validate an LDAP user log on action with one of the Content Manager EE clients to confirm that LDAP users can log on to the Content Manager EE clients.

To integrate and validate LDAP with your Content Manager EE system, use the following steps.

1. "Verifying the LDAP prerequisites"
2. "Generating the properties file"
3. "Testing the LDAP connection by searching for an LDAP user with the manual import function" on page 441
4. "Installing the properties file on the library server" on page 442
5. "Installing the properties file on the resource manager" on page 443
6. "Importing and synchronizing LDAP users and user groups with the LDAP user import utility" on page 444
7. "Installing the user exit for LDAP authentication" on page 451
8. "Installing prerequisite software for LDAP user authentication" on page 452
9. Optional: "Enabling SSL for LDAP server communication" on page 453
10. "Validating an LDAP user logon" on page 455

Related reference

"Troubleshooting LDAP integration" on page 666

Verifying the LDAP prerequisites:

Before you begin the steps to integrate LDAP with Content Manager EE, you must ensure that the prerequisite hardware and software are correctly installed.

See the information about hardware and software prerequisites for Content Manager EE. Work with the other members of your team, including the Content Manager EE installation team and the LDAP administrator, to ensure that all LDAP prerequisites are correctly installed and configured.

Related reference

Hardware and software requirements for Content Manager EE

Generating the properties file:

The `cmcmenv.properties` file is used by the system administration client utility program for importing users from the LDAP server. The library server and the resource manager might also require this file for user authentication, based on the configuration of your system.

To set up the information required to generate the properties file:

1. Start the system administration client.
2. Click **Tools > LDAP Configuration**.
3. Select the **Enable LDAP User Import and Authentication** check box.
4. Click the **Server** tab.
5. To supply the values to generate the properties file, enter data for the LDAP configuration options on the Server page. See the topic about defining the LDAP configuration for additional information about these options.

Tip: Supplying information in the Advanced and Authentication pages is an optional step. Those pages contain default LDAP configuration values that are sufficient for most content management systems.

When you save the LDAP configuration options, a `cmcmenv.properties` file is generated in the directory pointed to by the `IBMCMROOT/CMGMT` environment

variable on the system. In the next step of the LDAP integration, you test the properties of this file to ensure that it is configured correctly.

Related tasks

“Defining the LDAP configuration”

Defining the LDAP configuration:

The LDAP configuration contains values that are used by both the LDAP user import utility for automatic imports and the manual LDAP import. Values from the LDAP configuration are also used to generate the LDAP properties file.

The LDAP configuration contains data that is used to communicate with the LDAP server, including the LDAP server used, connection information for that server, and the distinguished name used to query objects on that server. The configuration also contains other data that defines how data is queried and imported when you are using the automatic or manual import. This data includes the LDAP attributes that become the Content Manager EE user name and user description, the scope of the search relative to the LDAP distinguished name used, and the number of records to retrieve. The configuration also includes options for setting up the Secure Sockets Layer (SSL) protocol to encrypt data imported from the LDAP server.

You set up the LDAP configuration as part of the LDAP integration steps. The data from the LDAP configuration is used to generate the LDAP properties file, `cmbcmenv.properties`, that is used on the system administration machine. The properties file might also be required on the library server and resource manager machines, depending on the configuration of your Content Manager EE system.

After you complete the LDAP integration for a content management system that is in production use, you might need to change the LDAP configuration data. For example, you might need to do the following tasks:

- Change the current default user attribute to a more useful one.
- Rescale the base DN (distinguished name) to include other areas of the LDAP hierarchical structure so that you can search for either a broader or narrower group of user IDs.
- Change the LDAP directory server host name so that the system administration client can import user IDs from a currently functioning LDAP directory server.

However, changing the LDAP configuration data generates a new LDAP properties file that contains the core LDAP configuration information. If you change the LDAP configuration for your production content management system after the initial LDAP integration is completed, then you must complete all steps in the LDAP integration process again. You must complete these steps to ensure that your content management system still functions correctly with LDAP.

Restriction: After the `cmbcmenv.properties` file is created, do not edit it directly. Always use the following procedure to update the file.

To define the LDAP configuration:

1. From the system administration client, click **Tools > LDAP Configuration** to open the LDAP Configuration window.
2. Select **Enable LDAP User import and authentication**.
3. Click the **Server** tab to configure the LDAP server information for use within Content Manager EE.

- a. In the **Server type** field, specify whether you want to import users from IBM Directory Server, Microsoft Active Directory, or other LDAP servers. Click **Active Directory** if you are using Active Directory. For other server types, click LDAP.
- b. In the **LDAP server Hostname** field, type the host name of the server from which you want to import users. Specify the host name by using the following format: `ldap://hostname.domain`.
- c. In the **Port** field, type the port number of the LDAP server. The default port numbers are 389 (non-Secure Sockets Layer) and 636 (Secure Sockets Layer). You can obtain more information about ports from your LDAP administrator.
- d. In the **Base DN** field, select the distinguished name that you want to use to query the objects in the LDAP server from the list.
DN is the distinguished name; an entry in the LDAP Directory Information Tree (DIT) that has one or more user attributes associated with it. You indicate a base DN as a place to begin queries for user IDs. For example, you can designate a base DN of User Accounts, which can contain several user attributes. When you search for user IDs to import, the search then looks for value matches in the user attributes of User Accounts, such as a user ID. You can obtain more information about the distinguished name to select from your LDAP administrator.

Tip: You can also click **Lookup from Server** to populate the list with all of the possible base DN's that are available from the server. However, the **Lookup from Server** selection might not work for your LDAP server. For most situations, you might want to input a base DN that you design to narrow the LDAP search scope.

- e. In the **User attribute** field, type the user attribute that is used to authenticate the user. The default user attribute for Content Manager EE is *cn* (common name). If you are using Microsoft Active Directory, change the user attribute to *samaccountname* so that Microsoft Active Directory verifies against the user ID instead of the common name. You can obtain a list of other user attributes from your LDAP administrator.

Important: The selection of the user attribute for this field is an important choice. This user attribute is used as the Content Manager EE User Name when the LDAP users are imported into the library server. Content Manager EE does not allow duplicate user names, so it is best to use an attribute that has a unique scope in the LDAP server, or one that appears as unique in the search scope that you configure as the filter for the LDAP search.

- f. In the **Description attribute** field, specify whether to use the distinguished name of the user as the description or another user attribute as the description after the user is imported to the system administration client.
- g. In the **Search scope** field, specify the level of your search. Click **One level** to limit the level of the search to users directly under the base DN or click **Subtree** to search for users in all branches under the base DN.
- h. In the **Referral** field, click **Follow** to forward the request to import users to another LDAP server that might be configured into your LDAP server. Click **Ignore** to import only users from the LDAP server that you defined.
- i. In the **Authentication scheme** field, notice that the system administration client specifies the Simple method to authenticate users.
- j. In the **User name** field, type the user name that allows you access to the users that you want to import. This user is not required to have

administrative privileges, but to avoid problems with denial of access, administrative privileges are strongly recommended.

Important: Some LDAP servers allow the use of the user name as the value for this field and other servers must use the full distinguished name (DN). For the best results for all servers, use the DN as the value for this field.

- k. In the **Password** field, type the password for the user name.
- 4. Optional: Click the **Authentication** tab to configure advanced authentication options. Advanced authentication options include enabling the Secure Sockets Layer (SSL) protocol. If you want to encrypt the data that you import from the LDAP directory server, complete the following steps.

Tip: If you are setting up LDAP integration for the first time to generate the properties file, then you can skip this step and complete it later. A later step in the LDAP integration process contains more complete instructions about how to enable SSL with the LDAP server.

- a. Select **Secure Sockets Layer (SSL) enabled**.
- b. Type the absolute path and name of an existing keyring file in the SSL keyring file field. The keyring file has an extension of kdb. For example:
`c:\absolute_path\keyringfile.kdb`
This file is just one of the pieces of information used to establish a secure connection to the LDAP directory server. The other piece of information required to establish a secure connection is the SSL authentication password.
- c. Type the password of the LDAP system administrator in the **SSL authentication password** field. You must have a valid LDAP system administrator password to connect to the LDAP directory server. Otherwise, any attempt to establish an SSL connection fails. Both the keyring file and password must contain trusted data to successfully connect to the LDAP directory server. If one of these objects has been tampered with or is no longer recognizable to the LDAP directory server, contact your LDAP system administrator for information to correct the problem.

Attention: The system administration client specifies the **Context Factory** to the SUN context factory. You cannot change this setting. Context factory is the underlying Java code used to connect the library server to the LDAP directory server.

- 5. Click the **Advanced** tab to configure the advanced server options.
 - a. In the **Max. records to retrieve** field, type the maximum number of user records to retrieve from a search. Ensure that this number is large enough to process all of the users and groups combined in the LDAP server to avoid errors when importing users with the LDAP user import utility.
You can check with your LDAP administrator to change the server configuration to return enough entries for the system administration client request. For example, Microsoft Active Directory, which is a part of Microsoft Windows 2000 Server, allows fetching only 1000 entries per one search request. The MaxPageSize parameter can be changed by using the ntdsutil.exe file on the Microsoft Windows 2000 Server machine. When you type ntdsutil in a command prompt, you must connect to your LDAP server first. Then, change MaxPageSize to the maximum number wanted and save your changes.

- b. In the **Server connection timeout** field, type the number of seconds to wait before you receive an error if the connection between the LDAP server and system administration client is not made. The maximum value is 99.

6. Click **OK** to save the changes.

Related tasks

“Importing and synchronizing LDAP users and user groups with the LDAP user import utility” on page 444

“Generating the properties file” on page 437

“Integrating LDAP with Content Manager EE” on page 436

Testing the LDAP connection by searching for an LDAP user with the manual import function:

After you generate the LDAP properties file, test the connection to the LDAP server by searching for an LDAP user with the manual user import process.

After you set up LDAP configuration data and generate the `cmbcmenv.properties` properties file, test that the properties are correctly configured to connect to the LDAP server. If you can find an LDAP user in the LDAP directory from the system administration client, then the properties file is correctly configured. To search for an LDAP user, you create a user and use the manual user import function as a search tool to find that user in the LDAP directory.

Tip: The process to import an LDAP user manually is available from the function to create a user in the system administration client. The manual method of importing users is convenient if you want to import only a few users. However, the LDAP user import utility is a more effective option if you need to import many users and user groups, such as when you are setting up LDAP for the first time. By using the LDAP user import utility, you can also set up a schedule to synchronize users and groups from the LDAP directory to the library server.

To test your connection to LDAP by searching for a user:

1. Expand **Authentication** in the system administration tree.
2. Right-click **Users** and click **New**. The New User window opens.
3. On the Define Users page, click **LDAP**. The Import users from LDAP window opens.
4. The **LDAP Server Hostname** field displays the host name of the LDAP directory server from which you are importing users. If you want to import users from an LDAP directory server other than the one that is listed, you must change the configuration by using the LDAP configuration tool.
5. Type the name of the user ID or user IDs that you want to find in the **Find users** field. For fuzzy searches, use the radio buttons to narrow your search.
 - To search for multiple users associated with the default user attribute, click the **User attribute** button. User attributes help describe the identity of the user. For example, the user attribute C identifies the country that the user operates from. You designate the default user attribute in the LDAP configuration tool.
 - To search for multiple users associated with an attribute other than the default attribute, click the **Other attribute** button and specify this attribute in the text field.

Tip: If you right-click in the **Other attribute** text field, a list of possible attributes displays. This list might not be the complete list of attributes available on the system. You can obtain a full list of valid user attributes from your LDAP administrator.

6. Click **Find** to conduct the search. The list of users retrieved from the search is displayed.

If the search finds the user, then the connection to LDAP is correctly configured. You can continue with the next step of LDAP integration.

If you choose to complete the import process for this test user, remember the following restrictions:

Restriction:

When you import LDAP user information, the LDAP user names must not contain the percent character (%), which the library server interprets as a search wildcard. For example, the user ID "j%smith" is not interpreted as a specific user ID. Instead, it is interpreted as "j" followed by any character, followed by "smith". If a user name contains the percent character, then the system administration client does not return the correct user properties when other user IDs match the pattern.

Important: If a distinguished name (DN) for a user changes later, you must reimport the user.

Installing the properties file on the library server:

If the library server is on a different machine than the system administration client, the library server requires the `cmbcmenv.properties` file for user authentication from the LDAP server.

If the library server is on a different machine than the system administration client, you must copy the generated `cmbcmenv.properties` file to the library server machine. You must copy the file into the directory that is pointed to by the `IBMCMROOT/CMGMT` environment variable. If there are multiple library server databases installed, you might want to copy it into a directory under `IBMCMROOT/CMGMT` with the same name as the database name. The library server LDAP user exit attempts to find this properties file under a directory with the database name that exists under the directory pointed to by the `IBMCMROOT/CMGMT` environment variable.

For example, on a UNIX system, if the library server database is `ICMNLSDDB`, then the library server attempts to find the `cmbcmenv.properties` file under the `IBMCMROOT/CMGMT/ICMNLSDDB` directory. Similarly on a Windows system, the library server looks under the `IBMCMROOT\CMGMT\ICMNLSDDB` directory.

If the properties file is not found in the directory with the database name under `IBMCMROOT/CMGMT`, the library server then looks for the file under the directory pointed to by `IBMCMROOT/CMGMT`.

To copy the properties file:

1. Back up the original properties file on the library server machine.
2. Copy the new properties file from the system administration client machine to the library server machine, into the directory with the matching name of the library server database. If there are multiple library server databases installed

on the same system, the directory that matches the library server database is the recommended place for the properties file.

Important: Transferring the file in the correct file format is critical, especially from a Windows system to a UNIX or Linux system. When you use an FTP tool to transfer the file, make sure that you transfer it with the ASCII format.

3. In the backup copy of the properties file for the library server, find and copy the line of code with the following parameter: CMCFGDIR. In most cases, this line is the first line of code in the file.
4. In the new properties file on the library server, replace the CMCFGDIR line of code with the copied line of code from the original file. The CMCFGDIR parameter is used by IBM Content Manager, not by LDAP, and the value on the library server must be the value from the original file.
5. For the Solaris platform with an Oracle library server database, you must complete the following additional steps in the new properties file:
 - a. Open the cmcmenv.properties file.
 - b. Find the line that begins with LDAP_PROVIDER_URL.
 - c. Delete ldap://. For example, change LDAP_PROVIDER_URL=ldap://cmi135.svl.ibm.com to LDAP_PROVIDER_URL=cmi135.svl.ibm.com.
 - d. Save the change.

Installing the properties file on the resource manager:

If you want to manage and authenticate the resource manager administrator ID through LDAP, then you must import the contents of cmcmenv.properties file into the RMCONFIGURATION table of the resource manager database. The default resource manager administrator ID is radmin.

The contents of the cmcmenv.properties file are imported into the RMCONFIGURATION table if the file exists in the required location and the resource manager application server is restarted. The file is imported every time that you restart the resource manager application server.

Important: After the LDAP configuration is initially imported to the resource manager, you might need to change the LDAP configuration on the resource manager. To make the changes to the LDAP configuration, you must delete the version of the cmcmenv.properties file that is on the resource manager. Then make the changes directly in the RMCONFIGURATION table. If you leave the incorrect cmcmenv.properties file on the resource manager, incorrect data is imported into the RMCONFIGURATION table the next time that the resource manager application server is restarted. To avoid a loss of the changes made to the LDAP configuration, always delete the properties file from the resource manager after the initial import and make any changes in the RMCONFIGURATION table.

Tip: If the resource manager is upgraded from Version 8.3, then the LDAP configuration is automatically migrated into the RMCONFIGURATION table.

To install the properties file on the resource manager and import the data into the RMCONFIGURATION table:

1. Copy the generated cmcmenv.properties file from the directory pointed to by the IBMCMROOT/CMGMT environment variable on the system administration client machine to the following directory on the resource manager. The following example shows the path for Windows:

`WAS_PROFILE_HOME\installedApps\node_name\icrm.ear\icrm.war\WEB-INF\classes
\com\ibm\mm\icrm`

In the path, the `icrm.ear` file name is the default resource manager application name (the installation default name).

2. Edit the `cmbcmenv.properties` file on the resource manager and change all encrypted passwords to clear text passwords.

Important: The change password request function in the LDAP server is not supported. You must use the administrative tool of the LDAP server (for example, the Directory Management tool of IBM Directory) to change the password yourself.

3. To import the properties into the `RMCONFIGURATION` table in the resource manager database, restart the resource manager application server.

Related tasks

“Configuring the resource manager for SSL communication with the LDAP server” on page 455

Importing and synchronizing LDAP users and user groups with the LDAP user import utility:

You use the LDAP user import utility to set up filter criteria and a schedule to import LDAP users and user groups. The schedule that you configure with the utility also synchronizes LDAP user IDs imported to the library server database with the users and user groups in the LDAP directory server.

The import process saves LDAP user names to the library server. A user name can be the common name, user ID, account name, email address, or other attribute of the LDAP user.

The LDAP user import utility automatically imports users and user groups defined in an LDAP directory into the Content Manager EE library server database. When you are importing many users, such as importing your users for the first time, the utility is more efficient than the manual import available in the user creation function. To use the LDAP user import utility, you define a set of filters for LDAP users and user groups and you create a schedule for the import task to run.

Users are automatically imported according to the schedule set in the utility. After the utility imports the users from LDAP for the first time, the utility synchronizes LDAP user IDs in the library server database with users and groups in the LDAP directory server. The utility synchronizes user additions, user deletions, and user transfers between user groups from the LDAP directory to the library server. The synchronization affects users and groups and the user-to-group relationship only. Those attributes should not be changed in the system administration client after the import from LDAP. The synchronization does not affect other attributes of users or groups. For example, Content Manager EE attributes related to privilege sets, default access control lists (ACLs), resource managers, and collections are not affected by the synchronization. You can change those attributes after the LDAP users are imported into the library server.

The synchronization does not affect users that are created with the system administration client or by using the APIs. For best results, do not mix users imported from LDAP users and groups with non-LDAP users and groups, or the synchronization process does not work as expected.

Restriction: For each machine on which the system administration client is installed, you can define only one LDAP import schedule for the database. In addition, if a user exists in the database, you cannot import the same user name from LDAP.

Restriction:

When you import LDAP user information, the LDAP user names must not contain the percent character (%), which the library server interprets as a search wildcard. For example, the user ID "j%smith" is not interpreted as a specific user ID. Instead, it is interpreted as "j" followed by any character, followed by "smith". If a user name contains the percent character, then the system administration client does not return the correct user properties when other user IDs match the pattern.

Important: If a distinguished name (DN) for a user changes later, you must reimport the user.

To define the import schedule for importing and synchronizing LDAP users and user groups:

1. Start the LDAP user import utility by completing the following step, as appropriate for your operating system.

Option	Description
Windows	Click Start > All Programs > IBM Content Manager > LDAP user import scheduler
AIX, Solaris, Linux	Use the following steps: <ol style="list-style-type: none"> 1. Change to the <i>IBMCMROOT</i>/admin/common/ directory, where <i>IBMCMROOT</i> is the installation path for the system administration client. 2. Ensure that the <i>IBMCMROOT</i> environment variable is correctly configured. 3. Enter the following command: ./cmldapimptool81.sh

Remember: When you start the LDAP user import utility, the **LDAP Directory (source)** area of the window contains LDAP server information that was provided during LDAP configuration. You cannot change the LDAP configuration from the LDAP user import utility. This information can be changed only by editing the LDAP configuration.

2. In the **LDAP object class for group** field, type the name of the entry in the LDAP directory that contains groups. Use any LDAP browser tool or run the **ldapsearch** command to find this information in the LDAP server. The following example shows the **ldapsearch** command on Windows, where *hostname* is the host name of the directory server, *bind_DN* is the bind distinguished name for accessing the directory, *password* is the password for the bind distinguished name, *base_DN* is the base distinguished name for the search operation, and *My_Group_Name* is the name of a user group:

```
ldapsearch -h hostname -D bind_DN -w password -b base_DN -R (cn=My_Group_Name)
```

For Tivoli Directory Server, the default group name is groupOfNames and for Microsoft Active Directory, the default value is group.

3. In the **LDAP attribute for group members** field, type the attribute for the group members. You can get the value for this field by using the LDAP browser or the **ldapsearch** command.

Tip: Dynamic groups, nested groups, and hybrid groups are supported with Tivoli Directory Server in IBM Content Manager Version 8.4 and later. To use these functions, you must choose a proper object class for the groups or use a top-level group to include all of those types of groups. For the **LDAP attribute for group members** field, you must use **all_members** to get all users from these special group types.

Important: Beginning with Version 8.4.2, IBM Content Manager supports nested groups for Microsoft Active Directory. To use this function, you can set the system environment variable **CMADNESTEDGROUPSUPPORT=YES** in the *IBMCMROOT\admin\common\cmldapimpusers81.bat* file or *IBMCMROOT\admin\common\cmldapimpusers81.sh* file that you use to import the users from the LDAP directory. You can also create the system environment variable **CMADNESTEDGROUPSUPPORT** and set it to a value of **YES** to enable this function.

4. In the **LDAP root DN** and **LDAP root DN password** fields, type the same values that were used for LDAP configuration. The LDAP user import scheduler uses these values to access the LDAP server and retrieve the user and group information.
5. The **Database** column lists the names of all IBM Content Manager and IBM Information Integrator for Content databases known to the system. Select the **Enable** check box for each database in which you plan to import LDAP users. Clear the check box if you do not want to import LDAP users into that database.
6. If the **Admin ID** field is blank, type the user ID of a user who has administrator privileges in that database. The **Admin ID** field is associated with the database and is needed for creating users and groups in the IBM Content Manager database. It is not used for importing users. If the ID has the privileges to create users in the database that you selected in the previous step, you can select another administration ID.
7. If the **Admin ID Password** field is blank, type the password for the administrator ID.
8. Click in the **User group** field for the selected database. The Group Policy window displays. Specify how user and group relationships should be imported into the database:
 - To create groups in the database that match the groups defined in the LDAP directory, click **Maintain the LDAP group names**. This action uses information specified in the **LDAP object class for groups** and **LDAP attribute for group members** fields to import LDAP data and correctly associate users with their respective groups.
 - To create a single group for all users, click **Place all users in one group** and then type the group name. In this case, the utility does not use the LDAP group name in the LDAP server.
 - To import users without associating those users to a group, click **No Group (Only import users)**.
 - To import users and associate the group name to a filter, click **Associate filters to group names**. You might use this feature when importing several groups and you want to change, or keep, the group name and associate that group name with a different privilege set. With this option, you can put any

set of users, defined by a filter, in a group that you name. Then you can assign any valid privilege set to those users.

Important: The LDAP user import scheduler imports users and groups and synchronizes the user-group relationships. When you specify a group name, do not use a group name that is already used for non-LDAP users in the IBM Content Manager database. Also, do not add a non-LDAP user to a group that contains LDAP users.

9. Click in the **Start time** field, and type the time of day for the utility to run. You must type the time by using the 24-hour clock, such as 09:30, 13:15, or 22:00. On the scheduled date and time, the utility updates the IBM Content Manager or IBM Information Integrator for Content database with current information from the LDAP directory.
10. Click in the **Day of week** field, select one or more days for the utility to run, and then click **OK**. On the scheduled date and time, the utility updates the IBM Content Manager or IBM Information Integrator for Content database with current information from the LDAP directory.
11. Click in the **User filter** field to define criteria to control which users get imported. The Filter(s) window displays. Specify the following values and then click **OK**. This field allows you to import specific users rather than all of the users that are defined in the LDAP directory.

Restriction: All the users and user groups that are selected for import in this step must be under the base distinguished name of the LDAP configuration. This value is the value that was supplied in the **Base DN** field during the LDAP configuration step.

- a. Select the type of filter that you want to use to define users. Select **User filter** to create a filter with user attributes or select **Group filter** to create a filter with group attributes. You can use more than one filter to define users, but you cannot mix user and group filters in the same filter definition.

Tip: For most content management systems, the type of import that you want to complete is an import of one or more LDAP user groups. Using the **Group filter** field instead of the **User filter** field can simplify the creation of filters for a user group import.

- b. In the **Enter filter for users** field, type the attributes to filter the users or groups. You can use the **ldapsearch** command or another LDAP search tool to validate this filter information.

Tip: Use the following examples and review the topic about filtering users for LDAP import if you need guidance on how to set up filters.

The following example shows a user filter for all users whose names start with the letters "j" or "k":

```
(&(objectclass=person)(|(cn=j*)(cn=k*)))
```

The following example shows a group filter for all users in group1 and group2:

```
(&(objectclass=group)(|(cn=group1)(cn=group2)))
```

- c. To associate a group with the users, type a group name in the **Name** field.

Restriction: This field is enabled only if you selected **Associate filters to group names** in the Group Policy window.

- d. To associate a privilege set with the users defined by the filter, type a privilege set name in the **Privilege Set** field. Ensure that the privilege set that you change to is already defined in the IBM Content Manager or IBM Information Integrator for Content database. All of the users that are defined by this filter are imported with the privilege set that is defined here. The default privilege set assigned to imported users is CLIENTUSERREADONLY.
 - e. Click **Add filter** to add this filter to the filter list and define another filter.
 - f. Click **OK** to save the values you specified and close the window, or **Cancel** to clear all the values you specified.
12. Click **Save** to save the values you specified and schedule the import utility to run.

After you set up the import schedule with the LDAP user import utility and save it, the import task is placed in the operating system as a scheduled task. Each time that the import schedule is saved or updated by using the LDAP user import utility, the previously saved import task is deleted from the list of scheduled tasks and is replaced with the new import task.

The import task runs at the time that is configured by the schedule. However, if you must start the import task manually with the data defined in the import schedule, you can run a batch or shell script to start the task. Use the following commands to run the import task manually, where *IBMCMROOT* is the installation path for the system administration client, *database_name* is the library server database name, and *server_type* is the server type, with a value of ICM for Content Manager EE and FED for IBM Information Integrator for Content.

```
Windows: IBMCMROOT\admin\common\cmldapimpusers81.bat database_name
server_type
AIX, Linux, Solaris: IBMCMROOT/admin/common/cmldapimpusers81.sh
database_name server_type
```

The following example is a command for an AIX, Linux, or Solaris system, where the library server database name is ICMNLSDB and the server type is ICM:

```
IBMCMROOT/admin/common/cmldapimpusers81.sh ICMNLSDB ICM
```

When you save the import schedule, the configuration data saves to the *IBMCMROOT/cmgmt/cmbinfo.ini* file. This file is used for debugging purposes if needed. Do not edit this file.

Related concepts

“Filtering users”

“LDAP user import utility usage notes” on page 449

“Identify the LDAP Directory Source” on page 450

Related tasks

“Defining the LDAP configuration” on page 438

“Manually importing user IDs from an LDAP directory server” on page 456

Filtering users:

When importing LDAP users, you can include or exclude users whose LDAP attributes satisfy the filter criteria. This feature makes it easy to import specific users rather than all of the users defined in the LDAP directory.

The filter syntax, which conforms to RFC 2254, is a logical expression that uses prefix notation (the operator must occur before the arguments being evaluated). For example, the following filter would import only those users who belonged to the organizationalPerson object class and had family names beginning with the letter R, S, or T:

```
(&(objectClass=organizationalPerson)(|(sn=R*)(sn=S*)(sn=T*)))
```

Use the following table as a guideline for entering user filter criteria.

Table 80. User filters

Filter	Symbol	Description	Example
Approximate	~=	The LDAP attribute value can match the filter criterion exactly or match variations in spelling.	(sn~=Jones)
Equality	=	The LDAP attribute value must match the filter criterion exactly.	(sn=Jones)
Greater than or equal	>=	The LDAP attribute value must match or be greater than the filter criterion.	(sn>=Jones)
Less than or equal	<=	The LDAP attribute value must match or be less than the filter criterion.	(sn<=Jones)
Presence	=*	The LDAP attribute must exist, such as all entries with the family name attribute.	(sn=*)
Substring		The LDAP attribute value must contain, begin with, or end with the filter criterion.	(sn=J*) (sn=*on*) (sn=Jo*n*)
And	&	Joins two expressions. A user entry in the LDAP directory must meet both criteria.	(&(sn=Jones)(ou=People))
Or		Joins two expressions. A user entry in the LDAP directory can match either criterion.	((sn=Jones)(sn=Smith))
Not	!	The LDAP attribute value cannot match the filter criterion.	!(sn=Jones))

Related tasks

“Importing and synchronizing LDAP users and user groups with the LDAP user import utility” on page 444

LDAP user import utility usage notes:

Review the LDAP user import utility usage notes for important information that can help you run the LDAP user import utility more effectively.

You must run the LDAP user import utility on the same machine on which the system administration client is installed. The LDAP server configuration for the system administration client is saved in the local copy of the cmbscmenv.properties file. The file is located on the machine where the system administration client is installed.

Restriction: You can define only one LDAP import schedule for each database, which is on the server that contains the system administration client.

- When the utility runs, groups and users that satisfy the filter criteria are added to the Content Manager EE or IBM Information Integrator for Content database only if they do not exist in the database or if the database does not reflect the same group and user mapping as the LDAP directory.
 - If you chose to maintain the LDAP groups, users are added into groups of the same name in the database.
 - If you chose to put all users in one group, all users are added to a single group in the database.
 - If you use the system administration client to modify a group or user record in the database, the import utility does not alter those changes. Be aware, however, that if you move a user from one group to another in the database, the import utility re-creates the user in a group that matches the user's association in the LDAP directory.
- If a group or user was deleted from the LDAP directory, the import utility deletes the group or user from the Content Manager EE or IBM Information Integrator for Content database.
- If an administrator uses the system administration client to delete a user from the Content Manager EE or IBM Information Integrator for Content database, the user is not deleted from the LDAP directory. Furthermore, unless you explicitly delete the user from the LDAP directory, or modify the user filter criteria to exclude that user, the user is re-created the next time that the import utility runs. This same processing occurs for groups that you delete from the Content Manager EE or IBM Information Integrator for Content database and then reimport from the LDAP directory.
- For Windows servers: To view a list of all tasks scheduled by the LDAP user import utility, open a command window and enter at the prompt. Any task created with this utility shows `cmldapimpusers81.bat` in its path. For Linux servers, open a terminal and enter `crontab -l`. Any task created with this utility shows `cmldapimpusers81.sh` in its path.
- To view information about import tasks that have already run, see the following log files:

Windows

`cmldapimpusers81.log`.

UNIX `cmldapimpusers81.stderr` and `cmldapimpusers81.stdout`.

- If the distinguished name (DN) for a user changes later, you must re-import the user.

Related tasks

“Importing and synchronizing LDAP users and user groups with the LDAP user import utility” on page 444

Identify the LDAP Directory Source:

The information displayed in the **LDAP Directory (Source)** area of the LDAP user import utility is obtained from the `cmmbcmenv.properties` file.

This file is populated during the installation of a Content Manager EE or IBM Information Integrator for Content system. It shows basic information about your LDAP server, such as the host name, port number, authentication protocol, and search base distinguished name (DN). Some of this information is provided for review purposes only; you cannot change it.

You must provide the following information or accept the default values.

LDAP object class for groups

Type the name of the object class that is used in your LDAP directory schema to identify an entry as a group definition, such as `groupofUniqueNames`. This information enables the LDAP user import utility to identify which entries in the directory constitute groups.

LDAP attribute for group members

Type the name of the attribute that is used in your LDAP directory schema to identify unique members of the group, such as `uniqueMember`. This information enables the LDAP user import utility to map users to their respective groups.

Root DN

Type the DN of the root user of the LDAP directory, such as `cn=root`. This information enables the LDAP user import utility to access the directory and read or update information in it. If you need assistance, consult your local LDAP administrator.

Root DN password

Type the password for the root DN.

Related tasks

“Importing and synchronizing LDAP users and user groups with the LDAP user import utility” on page 444

Installing the user exit for LDAP authentication:

The `ICMXLSLG.DLL` user exit sends user information to the LDAP server for authentication.

By default, the `ICMXLSLG.DLL` user exit is in an `ldap` directory under the directory pointed to by the `IBMCMROOT` environment variable. You must install the user exit in the correct location.

To install the user exit:

1. From the `ldap` directory, find the correct user exit DLL file to use for your content management system. The directory contains two DLL files.

Option	Description
ICMXLSLG.DLL	Choose this file if the library server is not enabled for Unicode.
ICMXLSLG.DLL.UNICODE	Choose this file if the library server is enabled for Unicode.

Important: The two DLL files that are available for selection are either 32-bit or 64-bit files, according to the operating system of the library server.

2. After you find the correct file, rename it to `ICMXLSLG.DLL` if necessary. The library server recognizes only `ICMXLSLG.DLL` as the name for this user exit.
3. Copy the `ICMXLSLG.DLL` LDAP user exit DLL from the `ldap` directory into the `PATHICMDLL/DBNAME/` directory.

The value for `DBNAME` is the database name. The value for `PATHICMDLL` can be determined by running the following DB2 Universal Database commands:

```
db2 connect to ICMNLSD user icmadmin using password
db2 select PATHICMDLL from icmstsyscontrol
```

For Oracle, use a similar command to determine the *PATHICMDLL* value.

Important: When copying the ICMXLSLG.DLL file, remember to preserve the uppercase characters in its name.

4. For UNIX only: Set the permission on the copied DLL. For example, if the *DBNAME* is ICMNLSDB:

```
cd PATHICMDLL
cd ICMNLSDB
cp $IBMCROOT/ldap/ICMXSLG.DLL
chmod 555 ICMXSLG.DLL
```

Important:

- Make sure that the .profile for the icmadmin user and the /home/\$DB2INSTANCE/sql/lib/db2profile have been updated for the IBMCROOT/CMGMT environment variable as directed by the procedures for your operating system.

Installing prerequisite software for LDAP user authentication:

The IBM Directory client SDK is prerequisite software for LDAP user authentication. If you plan to use Secure Sockets Layer (SSL) with your LDAP user authentication, then you must install the Global Security Kit (GSKit) as another prerequisite.

Regardless of the type of LDAP server that you are using in your content management system, the following prerequisite software must be installed to enable LDAP user authentication functions. If the prerequisite software was not installed during the Content Manager EE installation or upgrade, then it must be installed as part of the LDAP integration steps.

Install the prerequisite software on the same machine as the library server. The software contains libraries that the ICMXSLG.DLL user exit must use during authentication tasks with the LDAP server.

Tip: The IBM Tivoli Directory Server documentation contains complete instructions for installing these prerequisites. See the *IBM Tivoli Directory Server Installation and Configuration Guide* that is included with the code package or in the IBM Tivoli Information Center for these instructions.

To install the prerequisite software for LDAP user authentication:

1. Confirm the correct version of the IBM Tivoli Directory Server client to install by viewing the hardware and software prerequisites for Content Manager EE. The version that you install is dependent on the hardware and software platform of Content Manager EE and the database type of the library server.
2. Choose and install the correct IBM Tivoli Directory Server package. The package might contain code for several IBM Tivoli Directory Server features, including the server, client, GSKit, and others. Install the c-client feature to install the client.

Restriction: Do not install the IBM Tivoli Directory Server server.

3. Optional: If you want to use Secure Sockets Layer (SSL) with your LDAP user authentication process, install the IBM Tivoli Directory Server GSKit. Always use code from the same code package if you are installing both the GSKit code and the c-client code for IBM Tivoli Directory Server.

Related reference

Hardware and software requirements for Content Manager EE

Related information

 IBM Tivoli Information Center: IBM Tivoli Directory Server Installation and Configuration Guide

Instructions for Linux with an Oracle database only: IBM Tivoli Directory Server Version 6.1 client:

To support LDAP user authentication for Content Manager EE on Linux with a library server that uses the Oracle database, you must manually install the Content Manager EE IBM Tivoli Directory Server V6.1 client base package and its 32-bit library. Complete the following steps:

1. Enter the following commands:

```
tar xf tds61-linux-x86-64-CD1_w_entitlement.tar
cd tdsV6.1/tdsfiles
rpm -ivh idsldap-cltbase61-6.1.0-0.x86_64.rpm
rpm -ivh idsldap-clt32bit61-6.1.0-0.x86_64.rpm
```

2. Make sure that `/usr/lib/libibmldap.so` is successfully linked to the 32-bit library in the `/opt/ibm/ldap/V6.1/lib/libibmldap.so` path. If not, go to the `/opt/ibm/ldap/V6.1/lib/` path and enter `idslink -l 32 -f` to set up all links for the 32-bit library.

Enabling SSL for LDAP server communication:

For added security, you can configure Secure Sockets Layer (SSL) for LDAP user authentication.

Use this procedure for Windows, AIX, or Solaris operating systems.

Important: If the library server is on a Linux operating system and you want to use the LDAP user import and authentication function, do not enable SSL during the LDAP configuration. The SSL function for LDAP on Linux is not supported. Open the `cmbcenv.properties` file and make sure that `LDAP_SECURITY_PROTOCOL=none` instead of `LDAP_SECURITY_PROTOCOL=ssl`.

There are four steps required to configure SSL for LDAP user authentication.

1. "Creating the key database file"
2. "Configuring the system administration client for SSL communication" on page 454
3. "Configuring the library server for SSL communication with the LDAP server" on page 455
4. "Configuring the resource manager for SSL communication with the LDAP server" on page 455

Creating the key database file:

The first step to enable SSL for LDAP is to create the key database file. You must start the `ikeman` utility.

The LDAP server must be configured for SSL by using the Server Authentication method only. The Server and Client Authentication method is not supported.

Use the following steps to create the key database file:

1. Export the SSL certificate from the LDAP server in either Base64-encoded ASCII data or Binary Der data formats.
2. Start the ikeyman utility.
You can start this utility from either of the following locations:
 - GSKit software (for example, the gsk7ikm.exe file for GSKit 7)
 - IBM HTTP server
3. From the Key Database File menu, select **New**.
4. For **key database type**, enter: CMS key database file.
5. In the **File Name** field, enter a name for your key database file (for example: ldapkey.kdb).
6. In the **Location** field, enter: c:\Program Files\IBM\CMGMT (or any location on the local disk).
7. Click **OK**.
8. Enter a password.
9. In the Signer Certificates window, click **Add**.
10. Enter the name and location of the previously exported LDAP SSL certificate.
11. Click **OK**.
12. Copy the generated *ldapkey_name.kdb* file into the directory pointed to by the *IBMCMROOT/CMGMT* environment variable on the library server system.

Configuring the system administration client for SSL communication:

You must configure the system administration client to enable SSL for LDAP. Content Manager EE no longer configures SSL automatically.

Use these steps to configure the system administration client for SSL communication:

1. Start the system administration client.
2. Click **Tools > LDAP configuration**.
3. From the Authentication window, select **Secure Sockets Layer**.
4. Enter the name of the key database file that you created (for example: ldapkey).

Important: Do not add the .kdb extension to the file name in this field.

5. Enter the SSL authentication password in the **Password** field. Enter the password that you used when you created the key database file.
6. Click **OK**. This action updates the cmcmenv.properties file in the directory pointed to by the *IBMCMROOT/CMGMT* environment variable. If the library server is on a different system than the system administration client, you must copy the cmcmenv.properties file to the library server system.
7. Start the Java Runtime Environment (JRE) ikeyman utility program from the jdk/jre/bin directory and open the cacerts file by selecting the JKS format.
You can locate the jdk/jre/bin directory as follows:
 - If IBM Information Integrator for Content is installed on this system, navigate to the file in this location: *IBMCMROOT/jdk/jre/lib/security/cacerts*.
 - If IBM Information Integrator for Content is not installed on this system (only Content Manager EE), navigate to the file in this location: *IBMCMROOT/jdk/jre/lib/security/cacerts*.

8. Enter the password. If the file has not been changed, the default password is change it.
9. Add the exported SSL LDAP certificate into the cacerts file.
10. Restart the system administration client.

Configuring the library server for SSL communication with the LDAP server:

You must configure the library server to enable SSL for LDAP.

If the library server is on a different system than the system administration client, you must copy the properties file and the key database file to the library server system.

To complete the library server configuration for SSL with LDAP:

1. Back up the cmcmenv.properties file that is currently on the library server.
2. Copy the cmcmenv.properties file that was updated with the SSL information from the system administration client system to the library server system.
3. Copy and paste the line of code with the CMCFGDIR parameter from the backup properties file to the new properties file. See the information about installing the properties file on the library server for additional information about the CMCFGDIR parameter.
4. Copy the key database file (ldapkey.kdb) into the directory pointed to by the IBMCMROOT/CMGMT environment variable.

Related tasks

“Installing the properties file on the library server” on page 442

Configuring the resource manager for SSL communication with the LDAP server:

You must configure the resource manager to enable SSL for LDAP.

To configure the resource manager for SSL communication with the LDAP server, you must update the properties on the resource manager and add the SSL LDAP certificate.

To complete the resource manager configuration for SSL with LDAP:

1. Use the information for installing the properties file on the resource manager to move the updated properties file to the resource manager. After the changes for SSL, the settings from the updated cmcmenv.properties file on the system administration client must be added to the resource manager. However, you cannot simply copy the file from the system administration client to the resource manager. The LDAP integration step for installing the properties file on the resource manager has additional instructions about how to update the properties on the resource manager.
2. Add the exported SSL LDAP certificate into the following file:
`WAS_HOME\java\jre\lib\security\cacerts`
3. Restart the resource manager server.

Related tasks

“Installing the properties file on the resource manager” on page 443

Validating an LDAP user logon:

The final step of LDAP integration is to validate that an imported LDAP user ID can log on to one of the Content Manager EE clients.

To validate that an imported LDAP user can log on to a Content Manager EE client:

1. Select an imported user ID that you can access to use for the test.
2. Use one of the following options to test the user logon:
 - Use the user ID and password to log on to the eClient or Client for Windows.
 - Use the LDAP user preauthentication tool to test the logon. The LDAP user preauthentication tool is a command-line tool that helps you check that your LDAP integration is complete by authenticating an LDAP user to the Content Manager EE system.
3. If the log on is successful, then LDAP integration is complete. If the log on is not successful, then review the tasks performed in each of the integration steps. You can also see troubleshooting topics for LDAP for information that might help you solve the problem.

Related reference

“Troubleshooting authentication problems with the LDAP user preauthentication tool” on page 667

Manually importing user IDs from an LDAP directory server

The manual import function is a convenient method to use to import a single LDAP user or a few users into Content Manager EE.

The import process saves LDAP user names to the library server. A user name can be the common name, user ID, account name, email address, or other attribute of the LDAP user.

You use the manual import process to search for and import specific user IDs. You might want to use this method if you have several groups of user IDs with different security access.

The manual import function can also be used as LDAP user search function. For example, you can use the manual import to test your connection to the LDAP server. You can complete the steps in the manual import through the step where you click **Find** to find a user. If that user is found, then LDAP is configured correctly on your content management system.

The automatic import of LDAP users with the LDAP user import utility is a more convenient method to use if you are importing many LDAP users, such as during the initial setup of your LDAP users on Content Manager EE. The LDAP user import utility also enables you to synchronize user information from the LDAP directory server to the library server.

Restriction:

When you import LDAP user information, the LDAP user names must not contain the percent character (%), which the library server interprets as a search wildcard. For example, the user ID "j%smith" is not interpreted as a specific user ID. Instead, it is interpreted as "j" followed by any character, followed by "smith". If a user name contains the percent character, then the system administration client does not return the correct user properties when other user IDs match the pattern.

Important: If a distinguished name (DN) for a user changes later, you must reimport the user.

To import user IDs manually from an LDAP directory server:

1. Expand **Authentication** in the system administration tree.
2. Right-click **Users** and click **New**. The New User window opens.
3. On the Define Users page, click **LDAP**. The Import users from LDAP window opens.
4. The **LDAP Server Hostname** field displays the host name of the LDAP directory server from which you are importing users. If you want to import users from an LDAP directory server other than the one that is listed, you must change the configuration by using the LDAP configuration tool.
5. Type the name of the user ID or user IDs that you want to find in the **Find users** field. For fuzzy searches, use the radio buttons to narrow your search.
 - To search for multiple users associated with the default user attribute, click the **User attribute** button. User attributes help describe the identity of the user. For example, the user attribute C identifies the country that the user operates from. You designate the default user attribute in the LDAP configuration tool.
 - To search for multiple users associated with an attribute other than the default attribute, click the **Other attribute** button and specify this attribute in the text field.

Tip: If you right-click in the **Other attribute** text field, a list of possible attributes displays. This list might not be the complete list of attributes available on the system. You can obtain a full list of valid user attributes from your LDAP administrator.

6. Click **Find** to conduct the search. The list of users retrieved from the search is displayed.
7. Select the users that you want to import from the list and click **OK**. The Import users from LDAP window closes, returning you to the New User window.
8. In the New User window, select a privilege set in the **Privilege set** list for the user IDs listed in the **User Name** field.

Restriction: For each New User window that you open, you can assign only one privilege set to the user IDs that you import.

9. Click the **Set Default** tab to make sure that all defaults are selected.
10. Click **OK** or **Apply** to import and save the settings for these user IDs.

After you import the user IDs and save their access privileges, you can modify individual user ID access by viewing the properties. If these user IDs share similar access privileges or job responsibilities, you can group them together. Grouping user IDs is a convenient way to find user IDs. User groups are especially helpful when you must modify user IDs quickly or when you have many user IDs to manage.

Related tasks

“Importing and synchronizing LDAP users and user groups with the LDAP user import utility” on page 444

Creating users

A user ID must be created on each library server.

Each library server has a set of users who can access objects through it. You can limit a user's access to objects by assigning a privilege set when you create that

user. If a user must access more than one library server within the IBM Content Manager system, you must create a user ID on each library server that the user must access. The user ID can be the same on every server, but each user ID must be unique within one library server.

Tip: When you create a user ID, the system automatically assigns it to a predefined user group called, ICMPUBLIC. So, if you want to see all user IDs defined to the system, you can view this user group.

To create a user ID:

1. Expand **Authentication** in the tree view.
2. Right-click **Users** and click **New**. The New User window opens.
3. On the Define Users page, in the **User name** field, type:
 - up to 32 alphanumeric characters for the user ID if the database is on Windows
 - one to eight alphanumeric characters if the database is on z/OSUser IDs are not case-sensitive and can contain NLV characters. Optional: Click **LDAP** to import users stored in the LDAP directory server into your system.
4. Type a user description to help you identify the user. If you have configured your LDAP server, you can use the user description that the LDAP server has for user IDs by selecting the **Obtain from LDAP** check box.
5. If administrative domains are enabled, in the **Domain** list, select a domain to which the user belongs. For example, PUBLIC or RESTRICTED.
6. Select the **Use system password** check box if you want the password for this user to be the password defined for the operating system. Select this check box only if you want this user to be a superadministrator. You do not need to assign a subadministrator an operating system password because they cannot change settings on the server. After selecting this check box, the **Password**, **Confirm password**, and **Password expiration** fields are disabled.
7. In the **Password** field, type 1 to 32 alphanumeric characters as the password. When you type this password, this field displays an asterisk (*) for each character. Re-type the password in the **Confirm password** field.
8. In the **Password expiration** field, click **At next logon** to specify that the password expires immediately when the user logs on. Click **After** and enter a number to specify that the password expires after a certain number of days. Click **Use system default time** to specify that the password expiration is controlled in the system defined table.
9. From the **Privilege set** list, select a privilege set to assign the user. (Privilege sets define a user maximum ability to use the system.) You cannot assign a privilege set to a user group. If you do not see an existing privilege set that applies to this user ID, you can create a privilege set by clicking **Create Privilege Set**. In the New Privilege Set Definition window, you can define a new privilege set to add to the privilege set list.
10. Click **OK** to save the new user information and close the window.

Requirement: If you have more than one resource manager connected to the library server, you must select the default resource manager where the new user stores objects.

Related reference

“Considerations for Turkish locale” on page 682

Enabling user mappings

You can use the User Mapping window to enable the mapping of an IBM Information Integrator for Content user ID and password to a corresponding content server user ID and password.

If user mapping is enabled, the user ID in the mapping table is used. If the mapping table does not contain a user ID, then the user uses the current IBM Information Integrator for Content user ID and password to access the content server. If the connection fails, the user is prompted for a user ID and password for the content server. If the connection is successful, the user ID and password are stored in the mapping table for future connections.

If user mapping is not enabled, the user is always prompted for a user ID and password to access the content server.

To enable user mapping, complete the following steps:

1. Select **Tools > User mapping**. The User Mapping window opens.
2. Click **Enable mapping** to enable user mapping.
3. Click **OK** to save the setting and close the window.

Viewing or deleting user mappings:

Use the User Mapping Viewer window to view or delete user mappings. To view user mappings, click **Tools > User mapping Viewer**.

To delete a user mapping:

1. Select the user mapping that you want to delete from the **Federated user mappings** list.

Option	Description
Federated user	Displays a list of federated user IDs.
Federated user mappings	Displays the content server user IDs that are mapped to the selected federated user ID.
Server	Lists the content servers associated with the federated user ID.
User ID	Lists the user IDs used for the content servers.

2. Click **Selected** from the menu bar.
3. Click **Delete**.

Viewing or modifying users

As your system progresses and changes, you also need to address the changing needs of user access.

Constantly evaluate the access needs of your users. They need the appropriate access to objects to accomplish their jobs. You might even need to restrict their access as their job responsibilities change.

Requirement: If you have more than one resource manager connected to the library server, then you must select the default resource manager where the new user can store objects.

To view or modify a user:

1. Expand **Authentication** in the navigation pane.
2. Click **Users** to display a list of users in the details pane.
3. Right-click a user and click **Properties**. The User Properties window opens.
4. On the Define Users page, the user ID displays. You cannot change it.
Optional: If you use LDAP to store user IDs, and want to use IDs for the users in your LDAP server, you can click **LDAP** and select the users that you want.
5. Optional: In the **User description** field, type a user description to help you identify the user. If your LDAP server is already configured, then you can use the user description from that server for user IDs by selecting the **Obtain from LDAP** check box.
6. If administrative domains are enabled, select a domain to which the user belongs from the **Domain** list. For example, select PUBLIC or RESTRICTED.
7. Optional: Select the **Use system password** check box if you want the password for this user to be the password defined for the operating system. Select this check box only if you want this user to be a superadministrator. You do not need to assign a subadministrator an operating system password because they do not change settings on the server. After this check box is selected, the **Password**, **Confirm password**, and **Password expiration** fields are disabled.
8. In the **Password** field, type 1 - 32 alphanumeric characters as the password. When you type this password, this field displays an asterisk (*) for each character. Retype the password in the **Confirm Password** field. If you are importing users from LDAP, do not specify a password here because the password resides on the LDAP server.
9. In the **Password expiration** field, click **At next logon** to specify that the password expires immediately when the user logs on. Click **After** and enter a number to specify that the password expires after a certain number of days. Click **Use system default time** to specify that the password expiration is controlled in the system defined table.
10. From the **Privilege set** list, select a privilege set to assign the user. If you do not see an existing privilege set that applies to this user ID, you can create a privilege set by clicking **Create Privilege Set**. In the New Privilege Set Definition window, you can define a new privilege set to add to the **Privilege set** list.
11. Click **OK** to save the new user information and close the window.

Copying users

Copying an existing user to create a new user can save time as you create your content management system users.

If you need to create multiple users with identical settings, you might want to change only the user ID and description. You can accomplish this task by copying current user settings.

Requirement: If you have more than one resource manager connected to the library server, then you must select the default resource manager where the new user can store objects.

To copy a user:

1. Expand **Authentication** in the navigation pane.
2. Click **Users** to display a list of users in the details pane.
3. Right-click a user and click **Copy**. The Copy window opens.
4. On the Define Users page, in the **User name** field, type up to 32 characters. User IDs are not case-sensitive. **Optional:** If you use LDAP to store user IDs, and want to use IDs for the users in your LDAP server, you can click **LDAP**, and select the users that you want.
5. **Optional:** In the **User description** field, type a user description to help you identify the user. If you have configured your LDAP server, you can use the user description that the LDAP server has for user IDs by selecting the **Obtain from LDAP** check box.
6. If administrative domains are enabled, in the **Domain** list, select a domain to which the user belongs. For example, PUBLIC or RESTRICTED.
7. **Optional:** Select the **Use system password** check box if you want the password for this user to be the password defined for the operating system. Select this check box only if you want this user to be a superadministrator. You do not need to assign a subadministrator an operating system password because they cannot change settings on the server. After selecting this check box, the **Password**, **Confirm password**, and **Password expiration** fields are disabled.
8. In the **Password** field, type 1 - 32 alphanumeric characters as the password. When you type this password, this field displays an asterisk (*) for each character. Retype the password in the **Confirm Password** field. If you are importing users from LDAP, do not specify a password here because the password resides on the LDAP server.
9. In the **Password expiration** field, click **At next logon** to specify that the password expires immediately when the user logs on. Click **After** and enter a number to specify that the password expires after a certain number of days. Click **Use system default time** to specify that the password expiration is controlled in the system defined table.
10. From the **Privilege set** list, select a privilege set to assign the user. If you do not see an existing privilege set that applies to this user ID, you can create a privilege set by clicking **Create Privilege Set**. In the New Privilege Set Definition window, you can define a new privilege set to add to the **Privilege set** list.
11. Click **OK** to save the new user information and close the window.

Resetting user passwords

If a user account becomes locked, the system administrator might have to reset a user password.

Depending on system configuration, user accounts are locked when a user makes too many login attempts with an incorrect password. A system administrator who has DB2 administrator access can unlock accounts by resetting the user password.

If users request that you reset their password or if you need to unlock their account, then you need to complete the following steps:

Restriction: You cannot rename a user ID. You must copy or create another user ID to change user IDs.

1. Expand **Authentication** in the navigation pane.
2. Click **Users** to display a list of users in the details pane.

3. Right-click a user and click **Properties**. The Users Properties window opens.
4. Change the password.
5. Click **OK** to save the information and close the window.

To enforce password syntax validation for IBM Content Manager users, you can customize a user exit. When the user exit library is deployed, IBM Content Manager recognizes it and invokes it to validate passwords. By default, the IBM Content Manager sample library server user exit (ICMPLSVP) enforces the following password rules:

Passwords should be at least eight characters.

Each password should contain at least one non-alphabetic character.

Recommendation: For more secure passwords, you should customize the user exit to follow these common password guidelines:

- Passwords should be at least eight characters.
- Each password should contain at least two alphabetic characters and at least one numeric or special character. In English, the valid alphanumeric characters include:
 - 52 alphabetic characters (uppercase and lowercase)
 - 10 numerals
 - 3 special characters, the underscore (_), the number sign (#), and the dollar sign (\$)
- Password should expire after 90 days.
- Each password should differ from the user's user ID and any reverse or circular shift of that user ID.
- New passwords should differ from the old password by at least three characters.
- Avoid using consecutive sequences, dictionary words, or other easily guessed passwords.
- Never write down or share passwords.

Also refer to your local system password policies for guidance in your organization.

Related tasks

"Defining and configuring a library server" on page 5

"Viewing or modifying the configuration parameters" on page 6

Related reference

"Client logon attempts causing lockouts" on page 660

System password validation

You can define a user exit in the IBM Content Manager system that forces more strict password validation.

When you define the ICMValidatePassword user exit, the system calls that user exit each time that you create a user or update a user profile. The system also calls the user exit when users change their passwords. The system then applies the password rules that you have defined. You can modify the user exit to enforce the following types of password requirements:

- Password length
- Password must contain at least one non-alphabetic character
- The password expiration time frame

Important: If you modify a system administrator password from the system administration client, the Client for Windows, or the eClient, the user exit is not applied.

To see examples of how to modify the user exit, see the user exit sample that is most appropriate for your environment in the %IBMCMROOT%\samples\server\exit directory:

icmplsvp.c

User exit sample in C source code.

lspuxcom.h

Common header file that contains elements such as user exit constants and prototypes.

icmplsvp.def

Standard .def file for Windows.

icmplsvp.exp

Standard .exp file for Windows.

icmplsvp.mak

Makefile for multiple platforms, such as AIX, Sun, Linux, and Windows.

For z/OS, the following additional samples are provided for z/OS

ICMMCOXT JCL

Compiles icmxlsvp.c.

ICMMLXLJ JCL

Links icmxlsvp.c.

ICMMHLVP

Links the control statement file.

Related tasks

“Specifying user exit routines” on page 172

Assigning users to a user group

You can assign a user to a user group when you create a user or after a user is created. You might want to add or remove users depending on how their privileges change. User groups do not restrict or give access to any user. User groups only provide a convenient method to group users with similar business functions and is a quick way for system administrators to find specific users.

Tip: A predefined user group, ICMPUBLIC, is available for all user IDs. The system automatically assigns all user IDs to this group. So, if you want to see all user IDs defined to the system, you can view this user group by right-clicking it and selecting **Properties**. Once the panel opens select the **Show all** button to view all users.

To assign a user to a user group, complete the following steps:

1. Open the properties of a current user or open a New User window.
2. Click the **Assign to Groups** tab.
3. From the **Assign the users to one or more groups** list, select the user group to associate with this user. You can select multiple user groups. All available user groups are shown. You can also search for a specific group by using the search button located below the list.

4. Optional: Click **Create a Group** to open the New User Group window or right-click an existing user group and select Properties. By using this function, you can create a user group to add to the **Assign the users to one or more groups** list.

Assigning users to a collection

To allow users to access collections, you assign a collection on a resource manager to a domain to which users have access.

To assign users to a collection:

1. Open the properties of a current user or open a New User window.
2. Click the **Set defaults** tab.
3. Select a default collection when the user stores any objects.

Assigning users to resource managers

To allow users to access a specific resource manager, you assign a resource manager to a domain to which users have access.

To assign users to a resource manager:

1. Open the properties of a current user or open a New User window.
2. Click the **Set defaults** tab.
3. Select a default resource manager when the user stores any objects.

Selecting defaults for the user

To select the default resource manager, collection, and access control list for the user:

1. Click the **Set Defaults** tab.
2. Select a resource manager from the **Default Resource Manager** list. This resource manager is the default when the user stores any object.
3. Select a collection from the **Default Collection** list. This collection is the default when the user stores any object.
4. Select an access list from the **Default Item Access Control List** list. This access list is the default when the user creates an item.

Creating user groups

Gathering user IDs into user groups allows you to organize a system with many user IDs.

Benefits of user groups include:

- Finding specific user IDs
- Simplifying access control (treating users who have similar access needs or job requirements)

Example: You have 100 users who need access to the same objects. You do not want to list 100 users on the access control list for each object. So, you create a user group for those 100 users. Then each time you create an access control list, you only need to include the name of that user group.

Tip: When you create a user ID, the system automatically assigns it to a predefined user group called ICMPUBLIC. So, if you want to see all user IDs defined to the system, you can view this user group.

To create a user group:

1. Expand **Authentication** in the tree view.
2. Right-click **User Groups** and click **New** to open the New User Group window.
3. In the **Name** field, type a user group name. Type a 1 to 32 character name for the new user group. The user group ID must be unique and cannot be the same as any user group name. Assign a meaningful name to remind you of the type of users that belong to this group.
4. Optional: Type a description to help you identify the user group. This field is especially useful if you have users that share common access needs but do not have similar jobs.
5. If administrative domains are enabled, select a domain to which the user group belongs from the **Domain** list. Administrative domains limit a user's access to certain types of resource manager objects. For example, if you are a system administrator who manages the content for two banks, then you want to create two domains: one domain to be accessible only by users from Bank A and the other domain to be accessible by users from Bank B.
6. Populate the **Find users like (case sensitive)** list. This list helps you to locate the user IDs in your system. You can only choose user IDs that appear in this list.
 - a. Type a user ID that you want to include in the user group in the **Find users like (case sensitive)** list.
 - b. Select the parameters of your search. You can search for users by user ID or description. You do not need to know the exact user ID or description. For fuzzy searches, use the radio buttons to narrow the search. Click **Find**.
 - c. Click **Show All** to return all users who are defined in your system. You can select the users you want from the list. Users do not require the same privileges to be in the same user group.

Attention: Showing all users could take a long time if many users are defined in the system.
7. Select users from the **Find users like (case sensitive)** list and click **Add** to include them in the **Selected users** list.
8. Optional: If you want to remove users from the **Selected users** list, select the users and click **Remove**.
9. Click **OK** to save the new user group and close the window. Click **Apply** to save new user group and keep the window open to create another user group. Click **Cancel** to close window without saving anything.

Managing users and groups

A user group contains one or more users. A user group can be added to only one domain and can never be included in the domain SuperDomain. Every IBM Content Manager belongs to the user group ICMPUBLIC, a system defined user group.

When you manage users and groups, you define how end users access, search, and work with documents on multiple content servers by creating user IDs and privileges. You restrict access to the data stored in the system by defining and assigning appropriate privileges to the users. Often, users with the same job description have the same or similar tasks, and therefore, the same access to objects

on your system. You can group users with common access needs together in a user group. However, you cannot nest user groups.

A user group is only a convenient grouping of individual users with similar tasks. A user group makes it easier to create access control lists for objects in your system. You do not assign a user group a privilege set.

Note: If you have domains enabled before you assign a user ID to a group, check to see if that user group is in a specific domain or the PUBLIC domain. Make sure that the user group is in the domain that you want your user ID to be in.

Viewing or modifying user groups

If you need to change, add, or delete user IDs, you also need to modify the user groups that contain them. Remember to check the current user groups when you make any updates to user access. Delete any users who do not belong in a group. By periodically checking your user groups, you maintain a clean and efficient system.

To view or modify a user group:

1. Expand **Authentication** in the navigation pane.
2. Click **User Groups** to display a list of user groups in the details pane.
3. Right-click a user group and click **Properties** to open the Properties window. The name of the user group is displayed. You cannot change it.
4. Optional: Type a description to help you identify the user group. This field is especially useful if you have users that share common access needs but do not have similar jobs.
5. If administrative domains are enabled, select a domain to which the user group belongs from the **Administrative Domain** list. Administrative domains limits a user's access to certain types of resource manager objects. For example, if you are a system administrator who manages the content for two banks, then you want to create two domains: one domain to be accessible only by Bank A and the other domain to be accessible by Bank B.
6. Populate the **Find users like (case sensitive)** list. You can only choose user IDs that appear in this list.
 - a. Type a user ID that you want to include in the user group in the **Find users like (case sensitive)** list.
 - b. Select the parameters of your search. You can search for users by user ID or description. You do not need to know the exact user ID or description. For fuzzy searches, use the radio buttons to narrow the search. Click **Find**.
 - c. Click **Show All** to return all users who are defined in your system. You can select the users you want from the list. Users do not require the same privileges to be in the same user group.

Attention: Showing all users could take a long period of time if many users are defined in the system.
7. Select users from the **Find users like (case sensitive)** list and click **Add** to include an individual user or **Add All** to include all users in the **Selected users** list.
8. Optional: If you want to remove users from the **Selected users** list, select a user and click **Remove** or click **Remove All** to remove all users.
9. Click **OK** to save your changes and close the window. Click **Apply** to save your changes and keep the window open. Click **Cancel** to close window without saving anything.

Copying user groups

Tip: Because you often copy a user group to create another user group with identical settings, you might only want to change the name and description.

To copy a user group:

1. Expand **Authentication** in the navigation pane.
2. Click **User Groups** to display a list of user groups in the details pane.
3. Right-click a user group and click **Copy** to open the Copy window.
4. In the **Name** field, type a user group name. Assign a meaningful name to remind you of the type of users that belong to this group. User group names can be one to eight alphanumeric characters.
5. Optional: Type a description to help you identify the user group. This field is especially useful if you have users that share common access needs but do not have similar jobs.
6. If administrative domains are enabled, select a domain to which the user group belongs from the **Domain** list. Administrative domains limits a user's access to certain types of resource manager objects. For example, if you are a system administrator who manages the content for two banks, then you want to create two domains: one domain to be accessible only by Bank A and the other domain to be accessible by Bank B.
7. Populate the **Find users like (case sensitive)** list. You can only choose user IDs that appear in this list.
 - a. Type a user ID that you want to include in the user group in the **Find users like (case sensitive)** list.
 - b. Select the parameters of your search. You can search for users by user ID or description. You do not need to know the exact user ID or description. For fuzzy searches, use the radio buttons to narrow the search. Click **Find**.
 - c. Click **Show All** to return all users who are defined in your system. You can select the users you want from the list. Users do not require the same privileges to be in the same user group.

Attention: Showing all users could take a long period of time if many users are defined in the system.
8. Select users from the **Find users like (case sensitive)** list and click **Add** to include them in the **Selected users** list.
9. Optional: If you want to remove users from the **Selected users** list, select the users and click **Remove**.
10. Click **OK** to save the new user group and close the window. Click **Apply** to save new user group and keep the window open to create another user group. Click **Cancel** to close window without saving anything.

Authorizing users

Authorizing users includes managing data access and defining privileges, privilege sets, and privilege groups.

User authorization and privileges

User authorization is the method of controlling which users can log on, create other users, have a particular type of access to specific items, and so on. The system administration client provides several authorization objects to accomplish this including privileges, privilege groups, privilege sets, and access control lists. If you administer a combined IBM Content Manager and IBM Information Integrator

for Content system sharing the same database, all of the authorization objects are common to both parts of the client. This section presents an overview of how user authorization works.

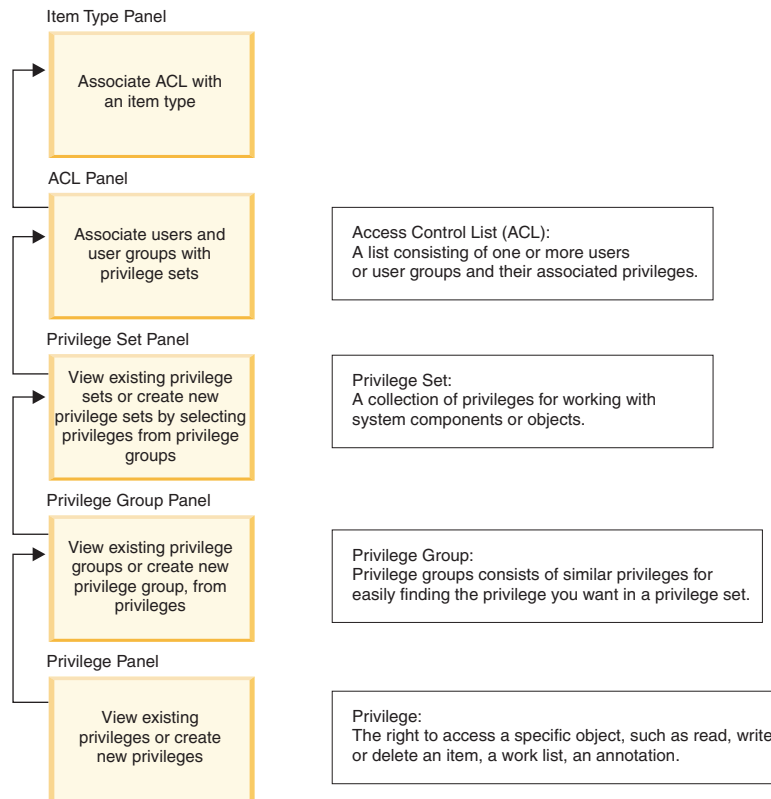


Figure 27. The relationship between privileges, privilege groups, privilege sets, and ACLs

Privilege

A privilege is the right to access a specific object in a specific way. Privileges include rights, such as being able to log on to a system, or create a user as well as reading, writing, or deleting an item, a worklist, or an annotation. Privileges represent individual user actions on objects. IBM Content Manager provides nearly 100 predefined privileges, including client privileges, item privileges, and system privileges.

Privilege group

A privilege group is simply a convenience grouping of similar privileges for the purpose of helping you create a privilege set. It represents a collection of user tasks. You only need to deal with privileges and privilege groups when you are creating new privilege sets. When you are creating a privilege set in the New Privilege Set Definition window, you can select a privilege group to see related privileges, and then add those privileges to the privilege set.

Privilege sets

A privilege set is a collection of privileges for working with system components and functions. For example, a privilege set gives authority to create users or log on a system. It represents a user role, like editor or reviewer. In the New User window, the assigned privilege set defines an

individual user's maximum ability to use the system objects. An access control list, however, might restrict an individual user's access to a particular object.

Access control lists

An access control list associates one or more user IDs (which includes its own privilege set) or user groups with privilege sets. User IDs might be associated with different privilege sets for different item types, so that they might be an editor for one item type and a reviewer for another item type. In the New Access Control List window, you can associate a privilege set with users or user groups. In the New Item Type Definition window of the Content Manager system administration client, you specify the access control lists to use for that item type. These access control lists can be used for multiple item types.

If you are planning to work with the data modeling objects, (if you want to define item types, for example) you must have both the DB2 privilege and an appropriate IBM Content Manager privilege. Administrators dealing with other objects need IBM Content Manager privileges, but not database administration privileges.

You can assign the UserDBConnect privilege set to a shared IBM Content Manager user ID for IBM Content Manager users who do not have individual database user IDs and passwords. IBM Content Manager uses this shared user ID to connect IBM Content Manager users to the database without requiring them to have their own database user IDs and passwords. By default, the shared IBM Content Manager user ID is ICMCONCT for Linux or Windows users.

You can also assign the UserDBTrustedConnect privilege set to the shared IBM Content Manager user ID. You can use this privilege set when a third party, such as an LDAP server, authenticates the IBM Content Manager user ID and password. After the IBM Content Manager user ID is authenticated, the IBM Content Manager user can log on to IBM Content Manager without a password.

Because worklists, work nodes, and processes are essentially items in IBM Content Manager, item related privileges are required to perform functions such as opening worklists and starting processes.

Authorizing user administrators to log on to the system administration client

In previous versions, only super users and, when administrative domains are enabled, domain users could log on to IBM Content Manager or IBM Information Integrator for Content system administration client. When these types of users logged on, the tasks that they could perform were not restricted to user or user group administrative tasks. Therefore, you could not create a user administrator whose function was only to administer users and user groups.

Now, the system administration client allows a user administrator with proper privileges to log on to the system administration client simply to administer users and user groups. The user administrator can view only the Authentication and Authorization nodes in the system administration client navigation tree.

Restriction: For the user administrator to successfully log on and define other users, the following requirements exist:

- The user administrator's privilege set must contain at least these privileges:

- SystemDefineUser
- SystemDefineGroup
- SystemQueryGroup
- SystemQueryUserPrivs
- SystemGrantUserPrivs
- The user administrator's task is to define other users and grant them privileges. Because the user administrator can grant other users only the privileges that the user administrator holds, additional privileges must be granted to the user administrator if the user administrator wants to grant additional privileges to other users.
- The user administrator can view only the Authentication and Authorization tree nodes in the navigation tree. The New User window displays only the names of the privilege sets. Therefore, the user administrator must use the Authorization tree node to view the available privileges contained within the privilege sets. If the user administrator attempts to perform a task in the Authorization tree node without proper privilege, an error message displays indicating that the user administrator does not have the privilege to perform the task.

These instructions provide an example explaining how a super user creates a user administrator, whose function is to create users with client privileges. In the example, the system administration client is installed on Windows and the library server database is DB2.

1. Create a system ID called client_user_admin on Windows.
2. Log on to the system administration client as a super user.
3. Create a privilege group called UserAdmin that contains the SystemDefineUser, SystemDefineGroup, SystemQueryGroup, SystemQueryUserPrivs, and SystemGrantUserPrivs privileges.
4. Create a ClientUserAdmin privilege set that contains privileges in both the UserAdmin and ClientTaskALL privilege groups.
5. Create a user called client_user_admin. Use the system password for the user ID and assign the ClientUserAdmin privilege set to the user.
6. Exit the system administration client.
7. Log on to the system administration client using the client_user_admin user ID. When this user administrator logs on, only the Authentication and Authorization nodes in the navigation tree are visible and the user can define users who have client privileges.

Managing access to data

A user cannot access the system without a user ID, password, and a privilege set. Before creating users and assigning them privilege sets, however, you must decide who has access to the system and what their jobs require. For example, you do not want users to have the right to delete an object when they do not understand the ramifications of deleting that object. Alternatively, you do not want to prevent users from doing their jobs by not giving them the correct privilege sets. So before assigning users privilege sets, you need to determine the types of tasks each job requires.

When users create objects, they must define the access that other users have to those objects and what operations can be done to the object. This definition is what is known to the system as an access control list, or an ACL.

Creating access control lists

An access control list (ACL) protects access to objects in your system by ensuring that only authorized users can access certain functions and stored objects.

An access control list consists of one or more user IDs or groups and associated privilege sets.

Restriction: If you enable administrative domains, you must belong to the SuperDomain to define access control lists or privilege sets. The SuperDomain is where you can manage system objects for all domains. If you do not belong to the SuperDomain, you can define access control lists or privilege sets if you assign the privilege to create access control lists or privilege sets to a domain. Access control lists and privilege sets can be associated with multiple domains, but they cannot be managed by users in any subdomains.

Requirement: When you create an ACL, you must have one or more privilege sets defined.

To create an access control list:

1. Expand **Authorization** in the tree view.
2. Right-click **Access Control Lists** and click **New**.
3. In the **Name** field of the new Access Control List window, type a unique and descriptive name.
4. Optional: Type a description to help you identify the access control list.
5. To include a user ID or group in the access control list:
 - a. To search by name, type a user or group name in the **Find groups/users** list and click the **Name** radio button. To search by description, type a user or group description and click the **Description** radio button.
 - b. You can search for users, groups, or both by selecting the **Users**, **Groups**, or **Both** radio button. You do not need to know the exact name or description. Case is ignored when searching by name, but respected when searching by description. For fuzzy searches, use the **Starting with**, **Containing**, and **Ending** radio buttons to narrow the search.
 - c. Click **Find**.
 - d. Click **Show All** if you do not know which users or groups to find. The system returns all users or user groups defined in your system.

You can select the users and groups that you want from the list. Users that are associated with a privilege set that contains the ItemSuperAccess privilege are not shown. This privilege bypasses access control list checking.

6. Optional: Use the fields below the **Find groups/users** list and the **Privilege Sets** list to search for a user or group, or for a privilege set. Type the first few letters of what you are looking for and click **Find**. The first result displays. By repeatedly clicking **Find**, you can display additional results one at a time.
7. Select one user or group and match it to one privilege set.
8. Click **Add** to include the pair in the **Users/Groups** list.
9. Optional: If you want to remove one or more pairings from the **Users/Groups** list, select the pair and click **Remove**.
10. Click **OK** to save any changes that you made to the access control list and close the window. Click **Apply** to save any changes and keep the window open to further modify the access control list. Click **Cancel** to close window without saving anything.

Access control lists: An access control list (ACL) is used as an additional check at run time to determine what create, retrieve, update, and delete operations a user can execute. An ACL is a list consisting of one or more individual user IDs or user groups and their associated privileges. You use ACLs to control user access to objects in the system. The objects that can be associated with access control lists are: the data objects stored by users, item types and item type subsets, worklists, and processes.

An assigned ACL restricts an individual user's access to an object, where an assigned privilege or privilege set defines the individual user's maximum ability to use the system. An ACL that has a privilege not included in a user's privilege set does not grant the user with that privilege. An ACL limits user access, it does not grant more access. ACLs provide another level of security when managing a system.

You can specify the access control list binding level in the IBM Content Manager system administration client New Item Type Definition Access Control window. If you select **Item type level**, then the access control list that you defined for an item type applies for all CRUD (create, retrieve, update and delete) operations of the items of that item type. If you select **Item level**, then the access control list for each item applies. If you change the access control list from the item level to the item type level, the item level ACLs are ignored.

One access control list, SuperUserACL, consists of a single rule that authorizes an IBM Content Manager preconfigured user, like ICMADMIN, to perform all IBM Content Manager functions. This access control list is not listed in the system administration client but can be assigned to entities, like an item type.

Any access control list (ACL) created by an IBM Content Manager administrator is called an *administrative ACL*. An IBM Content Manager administrator is a user who has system privileges SystemSetACL and SystemDefineACL. Administrative ACLs can be defined using the system administration client and are used with administrative objects, such as item types and item type views, or items.

Users with non-administrative privileges can define their own ACLs for use with items only. These ACLs are called *user ACLs*, and can be created by an end user with UserACLOwner privilege. Users can search on user ACLs. User ACLs do not display in the system administration client. A user who is listed in the user ACL and who has UserACLOwner privilege, or an administrator, can modify a user ACL using the APIs.

Restriction: To use the user ACL feature on z/OS, you must have the z/OS callable services interface, ICSF CSNBOW. This service is a base element of z/OS, but the ICSF callable services must be configured by a z/OS system administrator. For more information about setting up ICSF, see these sources:

- *z/OS ICSF Administrator's Guide (SA22-7521-07)*
- *z/OS ICSF System Programmer's Guide (SA22-7520-07)*

For more information on user ACLs, see the *Application Programming Reference* and *Application Programming Guide*.

Predefined access control lists:

The access control list (ACL) specifies who (users, groups, or public) can perform which functions (privileges) on a controlled entity. An ACL only defines the authorization of the bound entities and does not circumvent the user privileges.

The IBM Content Manager system provides the following pre-configured ACLs:

ACL	ACL definition
SuperUserACL	This ACL consists of a single rule that authorizes the IBM Content Manager pre-configured user (ICMADMIN) to perform all IBM Content Manager functions (AllPrivSet) on the bound entities.
NoAccessACL	This ACL consists of a single rule that specifies, for all IBM Content Manager users (Public), no actions (NoPrivSet) are allowed.
PublicReadACL	This ACL consists of a single rule that specifies, for all IBM Content Manager users (ICMPUBLIC), read operation (ItemReadPrivSet) is allowed. This is the default value assigned to the user's DfltACLCode.
RootFolderACL	This ACL manages access to the hierarchical root folder ICMROOTFOLDER, the root of all hierarchical folders in the content management system. This ACL can be used to manage the access of each user and user group to work with the ICMROOTFOLDER folder during item creation for a hierarchical item type. For example, you can authorize a group of users with a linking privilege set to enable items to be linked to the ICMROOTFOLDER folder. This ACL has no predefined rule. Therefore, an administrator must define the rules for this ACL if ICMROOTFOLDER is in use.
SysDefaultFolderACL	This ACL manages access to the system default hierarchical folder ICMSYSDEFAULTFOLDER. This ACL can be used to manage the access of each user and user group to work with the ICMSYSDEFAULTFOLDER folder during item creation for a hierarchical item type. For example, you can authorize a group of users with a linking privilege set to enable items to be linked to the ICMSYSDEFAULTFOLDER folder. This ACL has no predefined rule. Therefore, an administrator must define rules for this ACL if ICMSYSDEFAULTFOLDER is in use.

Related tasks

Creating a root hierarchical folder

Setting the default hierarchical folder

Viewing or modifying access control lists:

For security purposes, you need to regularly check the current access privileges that your access control lists provide.

You might need to update the access privileges in the access control lists. If you have administrative domains, you might need to move or delete access control lists.

To view or modify an access control list:

1. Expand **Authorization** in the navigation pane.
2. Click **Access Control Lists** to display a list of access control lists in the details pane.
3. Right-click an access control list and click **Properties**. The Access Control List Properties window opens. The name of the access control list is displayed. You cannot change it.

4. Optional: Type a description to help you identify the access control list.
5. To include a user ID or group in the access control list:
 - a. To search by name, type a user or group name in the **Find groups/users** list and click the **Name** radio button. To search by description, type a user or group description and click the **Description** radio button.
 - b. You can search for users, groups, or both by selecting the **Users**, **Groups**, or **Both** radio button. You do not need to know the exact name or description. Case is ignored when searching by name, but respected when searching by description. For fuzzy searches, use the **Starting with**, **Containing**, and **Ending** radio buttons to narrow the search.
 - c. Click **Find**.
 - d. Click **Show All** if you do not know which users or groups to find. The system returns all users or user groups defined in your system.

You can select the users and groups that you want from the list. Users that are associated with a privilege set that contains the ItemSuperAccess privilege are not shown. This privilege bypasses access control list checking.

6. Optional: Use the fields below the **Find groups/users** list and the **Privilege Sets** list to search for a user or group, or for a privilege set. Type the first few letters of what you are looking for and click **Find**. The first result displays. By repeatedly clicking **Find**, you can display additional results one at a time.
7. Select one user or group and match it to one privilege set.
8. Click **Add** to include the pair in the **Users/Groups** list.
9. Optional: If you want to remove one or more pairings from the **User/Groups** list, select the pair and click **Remove**.
10. Click **OK** to save any changes that you made to the access control list and close the window. Click **Apply** to save any changes and keep the window open to further modify the access control list. Click **Cancel** to close window without saving anything.

Deleting user access control lists:

You might need to delete a user access control list as part of regular maintenance of your content management system.

User ACLs that were created but never assigned to any item are considered orphan user ACLs. These ACLs can be removed from the IBM Content Manager server by the IBM Content Manager administrator by using a command-line tool.

- On Windows: *IBMCMROOT\config\cleanupUserACL.bat*
- On UNIX: *IBMCMROOT/config/cleanupUserACL.sh*

Follow this usage: `cleanupUserACL <db> <user> <pwd> <schema> <error file>`

where:

- *db* is the library server database name
- *user* is the library server administrator user ID
- *pwd* is the library server administrator password
- *schema* is the schema
- *error file* is the output messages

If you receive an Error cleaning user ACLs message, follow these steps to create a required `cmbicmsrvs.ini` file:

1. From a command window, change to the *IBMCMROOT*\bin directory.
2. Run cmbenv81.
3. Change to the *IBMCMROOT*\cmgmt\connectors directory or create it if it does not exist.
4. Run the following command, entered on a single line, and provide the name of the library server:

```
java com.ibm.mm.sdk.util.cmbsrvsictm -a add -s
library_server_database_name
```

This procedure creates a cmbicmsrvs.ini file in *IBMCMROOT*\cmgmt\connectors with the following data (in this case, *library_server_database_name* is icmnlbdb):

```
ICMSERVER=icmnlbdb
ICMSERVERREPTYPE=DB2
ICMSchema=ICMADMIN
ICMSSO=FALSE
ICMDBAUTH=SERVER
ICMREMOTE=FALSE
ICMHOSTNAME=
ICMPORT=
ICMREMOTEDB=
ICMNODENAME=
ICMOSTYPE=
ICMJDBCdriver=
ICMJDBCURL=
ICMJNDIREF=
ICMDBVER=
ICMGMTSYSATTRTS=
```

Restriction: If you are using Oracle 11g, then you must enter a JDBC type 4 connection string as the value for the ICMJDBCURL parameter in the cmbicmsrvs.ini file to use the cleanupUserACL tool. Type 2 connection strings are not supported. If you leave the value for this parameter blank, a type 2 connection string is used by default.

To see all optional parameters for com.ibm.mm.sdk.util.cmbsrvsictm, run this command: java com.ibm.mm.sdk.util.cmbsrvsictm

Related concepts

JDBC connection string support in Oracle

Copying access control lists:

Copying an existing access control list (ACL) to create a new list can save time as you create your ACLs.

When you find that access control lists that you need to create share similar properties, you can copy an existing ACL to create a new one. If you have enabled administrative domains, you can create similar access control lists and assign each one to a different domain.

To copy an access control list:

1. Expand **Authorization** in the navigation pane.
2. Click **Access Control Lists** to display a list of access control lists in the details pane.
3. Right-click an access control list and click **Copy**. The Copy Access Control List window opens.
4. In the **Name** field, rename the access control list.

5. Optional: Type a description to help you identify the access control list.
6. To include a user ID or group in the access control list:
 - a. To search by name, type a user or group name in the **Find groups/users** list and click the **Name** radio button. To search by description, type a user or group description and click the **Description** radio button.
 - b. You can search for users, groups, or both by selecting the **Users**, **Groups**, or **Both** radio button. You do not need to know the exact name or description. Case is ignored when searching by name, but respected when searching by description. For fuzzy searches, use the **Starting with**, **Containing**, and **Ending** radio buttons to narrow the search.
 - c. Click **Find**.
 - d. Click **Show All** if you do not know which users or groups to find. The system returns all users or user groups defined in your system.

You can select the users and groups that you want from the list. Users that are associated with a privilege set that contains the ItemSuperAccess privilege are not shown. This privilege bypasses access control list checking.

7. Optional: Use the fields below the **Find groups/users** list and the **Privilege Sets** list to search for a user or group, or for a privilege set. Type the first couple of letters of what you are looking for and click **Find**. The first result displays. By repeatedly clicking **Find**, you can display additional results one at a time.
8. Select one user or group and match it to one privilege set.
9. Click **Add** to include the pair in the **User/Groups** list.
10. Optional: If you want to remove one or more pairings from the **User/Groups** list, select the pair and click **Remove**.
11. Click **OK** to save any changes that you made to the access control list and close the window. Click **Apply** to save any changes and keep the window open to further modify the access control list. Click **Cancel** to close window without saving anything.

Defining privileges, privilege groups, and privilege sets

Privileges give system users, such as administrators and client users, the right, or rights, to act on a certain object in a certain way.

The system administration client provides predefined privileges, privilege groups, and privilege sets. You can also create your own privileges, privilege groups, and privilege sets. Privileges can be grouped in collections in two different ways, by using privilege groups and privilege sets.

Privileges

A *privilege* is the right to act on a certain object in a specific way. For example, you might assign the ItemAdd and ItemDelete privileges to client users to give them the right to add or delete items from a content server. To view privileges, expand **Authentication** and click **Privileges**. To create a privilege, right-click **Privileges** and click **New**.

Note: The provided IBM Content Manager clients rely on the system-defined privileges. New privileges are needed only if you create custom applications.

Privilege groups

A *privilege group* is a collection of related privileges. For example, the

privilege group named Administer Information Integrator for Content contains privileges typically associated with administering an IBM Content Manager system:

- EIPAdminServer
- EIPAdminEntity
- EIPAdminTextEntity
- EIPAdminTemplate
- EIPAdminInfoMining

To view the privileges preassigned to a privilege group, expand **Authentication > Privilege Groups**. Double-click the privilege group name or right-click the privilege group name and select **Properties**.

Privilege sets

Privilege sets are a collection of privileges that define user roles. For example, the privilege set named ClientUserCreateAndDelete contains 17 privileges associated with client user roles, such as Delete (delete an item), ItemAdd (add an item), and others. If you create a user ID for a client user and assign the privilege set ClientUserCreateAndDelete, the user can log in to a content server and perform any of the 17 user roles contained in the privilege set. To view privilege sets, expand **Authentication**, click **Privilege Sets**, and double-click a privilege set name.

Note: To avoid security problems, give users correct privileges or privilege sets. For example, giving a user the SysAdminSuper privilege set, composed of all privileges except AllowConnectToLogon and AllowTrustedLogon, allows the user to perform all system administration functions and have all client privileges. Misuse of granted privileges could result in data management problems or the assignment of more incorrect privileges.

Creating privileges

A privilege is the right to access a specific object in a specific way. Privileges include rights such as creating, deleting, and selecting objects stored in the system. Privileges represent individual user actions on objects. The system administration client has several system-defined privileges available. Sometimes, however, you have reasons to create your own privileges, such as instances when you create your own custom application.

To create a privilege:

1. Expand **Authorization** in the tree view.
2. Right-click **Privileges** and select **New**. The New Privilege Definition window opens.
3. In the **Privilege name** field, type a descriptive name for the privilege.
4. Optional: In the **Description** field, type a description that will help you identify the new privilege.
5. Click **OK** to save and close the window. Click **Apply** to save this privilege and create another privilege.

Predefined privileges:

The system administration client has nearly 100 system-defined privileges available. Each privilege can belong to one or more privilege sets.

The following areas include predefined privileges:

- “Allow privileges”
- “Client privileges”
- “EIPAdmin privileges” on page 483
- “Item privileges” on page 484
- “System privileges” on page 497
- “WF privileges” on page 505

Allow privileges:

The privileges starting with *Allow* are related to the log on properties of the IBM Content Manager users.

AllowConnectToLogon

Users with this privilege can log on to the library server by using the shared database connection ID ICMCONCT (on Linux or Windows). By using the shared connection ID, IBM Content Manager user IDs do not need to be defined in the operating system. By default, the database connection user ID already has this privilege and no other IBM Content Manager user needs this privilege. IBM Content Manager user IDs that use a shared connection to log on to IBM Content Manager do not require this privilege.

Used by	Connect users
Member of privilege sets	AllPrivs, UserDBConnect, UserDBTrustedConnect
Member of privilege groups	ClientTaskLogon
Required privileges	none
Related privileges	AllowTrustedLogon

AllowTrustedLogon

Users with this privilege can log on with a different database connection user ID and without a password. Both the database connection user and your own user ID must have this privilege.

Used by	Connect users
Member of privilege sets	AllPrivs, UserDBTrustedConnect
Member of privilege groups	ClientTaskLogon
Required privileges	none
Related privileges	AllowConnectToLogon

Client privileges:

The *Client* privileges, in conjunction with other privileges, are used by Client for Windows and eClient in validating client user authorization.

ClientAddNewBasePart

Users with this privilege can add a new base document part. You will be able to scan and import the documents.

Used by	Client users
----------------	--------------

Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskCreate, ClientTaskUpdate
Required privileges	ItemTypeQuery, ItemCheckInOut, and either ItemAdd or ItemAddPart
Related privileges	ClientModifyBasePart, ClientReadBasePart, ClientDeleteBasePart

ClientAddToNoteLog

Users with this privilege can add notes to a note log.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect, ItemCheckInOut, and either ItemSetUserAttr or ItemUpdatePart
Related privileges	ClientModifyNoteLog, ClientReadNoteLog

ClientAdvancedSearch

Users with this privilege can perform searches using the advanced search dialog.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskMinimum
Required privileges	ItemQuery, ItemSQLSelect, ItemTypeQuery
Related privileges	none

ClientDeleteBasePart

This privilege allows the user to delete a base document part.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect, ItemCheckInOut, and either ItemDelete or ItemDeletePart

Related privileges	ClientModifyBasePart, ClientReadBasePart, ClientAddNewBasePart
---------------------------	--

ClientExport

Users with this privilege can export any available document information.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll
Required privileges	ItemQuery, ItemSQLSelect, ItemTypeQuery, ClientReadBasePart
Related privileges	none

ClientGetWorkList

Users with this privilege can show the full list of documents and folders in system assigned worklists.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs
Member of privilege groups	ClientTaskAll
Required privileges	none
Related privileges	none

ClientImport

Users with this privilege can import a document.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskCreate
Required privileges	ItemTypeQuery, ItemAdd, ClientAddNewBasePart
Related privileges	ClientScan

ClientModifyAnnotation

Users with this privilege can modify an annotation.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper

Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect, ClientReadBasePart, ClientReadAnnotation, ItemCheckInOut, and either ItemSetUserAttr or ItemUpdatePart
Related privileges	ClientReadAnnotation

ClientModifyBasePart

Users with this privilege can modify base document part.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect, ClientReadBasePart, ItemCheckInOut, and either ItemSetUserAttr or ItemUpdatePart
Related privileges	ClientDeleteBasePart, ClientAddNewBasePart, ClientReadBasePart

ClientModifyNoteLog

This privilege allows the user to modify note log part.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect, ClientReadBasePart, ClientReadNoteLog, ItemCheckInOut, and either ItemSetUserAttr or ItemUpdatePart
Related privileges	ClientAddToNoteLog, ClientReadNoteLog

ClientPrint

Users with this privilege can print a document.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskView
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect, ClientReadBasePart, ClientReadNoteLog, ClientReadAnnotation
Related privileges	none

ClientReadAnnotation

Users with this privilege can view annotations.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskView
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect, ClientReadBasePart
Related privileges	ClientModifyAnnotation

ClientReadBasePart

Users with this privilege can view document base part.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskView
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect
Related privileges	ClientDeleteBasePart, ClientAddNewBasePart, ClientModifyBasePart

ClientReadHistory

Users with this privilege can view the history log of an item.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskView
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect
Related privileges	none

ClientReadNoteLog

Users with this privilege can view a note log part.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper

Member of privilege groups	ClientTaskAll, ClientTaskView
Required privileges	ItemTypeQuery, ItemQuery, ItemSQLSelect
Related privileges	ClientModifyNoteLog, ClientAddToNoteLog

ClientScan

Users with this privilege can scan a document or images.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskCreate
Required privileges	ClientAddNewBasePart, ItemAdd , ItemTypeQuery
Related privileges	ClientImport

EIPAdmin privileges:

The privileges starting with *EIPAdmin* pertain to administering IBM Information Integrator for Content. These privileges are useful only if you have IBM Content Manager installed. IBM Content Manager was formerly known as Enterprise Information Portal, or EIP.

EIPAdminEntity

Users with this privilege can administer IBM Content Manager federated entities, including the ability to create, modify, and delete.

Used by	IBM Content Manager administrators
Member of privilege sets	AllPrivs, SysAdminEIP, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerEIP
Required privileges	none
Related privileges	EIPAdminServer, EIPAdminTemplate, EIPAdminTextEntity

EIPAdminServer

Users with this privilege can administer IBM Information Integrator for Content content servers, including the ability to create, modify, and delete.

Used by	IBM Content Manager administrators
Member of privilege sets	AllPrivs, SysAdminEIP, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerEIP
Required privileges	none
Related privileges	EIPAdminEntity, EIPAdminTemplate, EIPAdminTextEntity

EIPAdminTemplate

Users with this privilege can have full control of the IBM Content Manager search templates, including the ability to create, modify, and delete.

Used by	IBM Content Manager administrators
Member of privilege sets	AllPrivs, SysAdminEIP, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerEIP
Required privileges	none
Related privileges	EIPAdminServer, EIPAdminEntity, EIPAdminTextEntity

EIPAdminTextEntity

Users with this privilege can administer IBM Content Manager federated text indexes, including the ability to create, modify, and delete.

Used by	IBM Content Manager administrators
Member of privilege sets	AllPrivs, SysAdminEIP, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerEIP
Required privileges	none
Related privileges	EIPAdminServer, EIPAdminTemplate, EIPAdminEntity

Item privileges:

Most of these privileges start with *Item*, and are for application runtime and document routing actions.

ItemAdd

Users with this privilege can create items or documents. This privilege is also needed in order to define (or add) a document routing process definition to the system.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskCreate, ClientTaskUpdate
Required privileges	none
Related privileges	ItemTypeQuery, ItemSetUserAttr, ItemDelete, ItemAddPart, ItemRouteStart

ItemAddLink

Users with this privilege can create a link between two items, either in the same item type or in different item types.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemLinkTo, ItemLinked, ItemCheckInOut
Related privileges	ItemAdd, ItemLinkTo, ItemLinked, ItemRemoveLink, ItemCheckInOut, ItemTypeQuery, ItemQuery, ItemSQLSelect

ItemAddToDomain

This privilege allow you to add an item to a domain.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll
Required privileges	ItemAdd
Related privileges	ItemAdd

ItemCheckInOut

Users with this privilege can check out or lock an item, or can check in or unlock an item that was checked out by a different user.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskCreate, ClientTaskUpdate
Required privileges	none
Related privileges	ItemSuperCheckInOut, ItemSetUserAttr, ItemSetSysAttr, ItemMove, ItemAddPart, ItemUpdatePart, ItemDeletePart, ItemAddLink, ItemRemoveLink, ItemTypeQuery, ItemQuery, ItemSQLSelect, ItemLinked, ItemLinkTo

ItemDelete

Users with this privilege can delete items and documents. This privilege is required to delete a document routing definition.

To delete an item and its associated parts, users need this privilege in their general privilege set and in the privilege set associated with the users in the access control list for the document and any associated parts.

Used by	Client users
----------------	--------------

Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	none
Related privileges	ItemAdd, ItemSQLSelect, ItemTypeQuery, ItemQuery, ItemRemoveLink

ItemDeletePart

Users with this privilege can delete resource parts of a document. If you only have this privilege and not ItemSetUserAttr, then you can only delete resource parts but not update the document's attributes.

To delete parts, users need the ItemDelete and ItemDeletePart privileges in their general privilege set and in the privilege set associated with the users in the access control list for the document and any associated parts.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemCheckInOut
Related privileges	ItemAddPart, ItemUpdatePart, ItemSetUserAttr, ItemTypeQuery, ItemQuery, ItemSQLSelect, ItemCheckInOut

ItemAddPart

Users with this privilege can add resource parts of a document. If you only have this privilege and not ItemSetUserAttr, then you can only add resource parts but not update the document's attributes.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemCheckInOut
Related privileges	ItemDeletePart, ItemUpdatePart, ItemSetUserAttr, ItemDeletePart, ItemTypeQuery, ItemQuery, ItemSQLSelect, ItemCheckInOut

ItemUpdatePart

Users with this privilege can update resource parts of a document. If you only have this privilege and not ItemSetUserAttr, then you can only update resource parts but not update the document's attributes.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemCheckInOut
Related privileges	ItemDeletePart, ItemAddPart, ItemSetUserAttr, ItemDeletePart, ItemTypeQuery, ItemQuery, ItemSQLSelect, ItemCheckInOut

ItemGetAssignedWork

Users with this privilege can retrieve work items assigned to another user. This privilege is related to work assignment in document routing.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll
Required privileges	none
Related privileges	ItemGetWork, ItemGetWorkList, ItemRoute, ItemRouteEnd, ItemRouteStart, ItemUpdateWork

ItemGetWork

Users with this privilege can retrieve work packages for document routing.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWorkList, ItemRoute, ItemRouteEnd, ItemRouteStart, ItemUpdateWork

ItemGetWorkList

Users with this privilege can retrieve worklists for document routing.

Used by	Client users
----------------	--------------

Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemRoute, ItemRouteEnd, ItemRouteStart, ItemUpdateWork

ItemLinked

Items with this privilege can have other users to add or delete links to the item.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemAddLink, ItemRemoveLink, ItemLinkedTo, ItemCheckInOut
Related privileges	ItemLinkTo, ItemAddLink, ItemRemoveLink, ItemDeletePart, ItemTypeQuery, ItemQuery, ItemSQLSelect, ItemCheckInOut

ItemLinkTo

Items with this privilege can have users add and remove links from the item.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemAddLink, ItemRemoveLink, ItemLinked, ItemCheckInOut
Related privileges	ItemLinked, ItemAddLink, ItemRemoveLink, ItemTypeQuery, ItemQuery, ItemSQLSelect, ItemCheckInOut

ItemMove

Users with this privilege can move items or documents between item types.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate

Required privileges	ItemCheckInOut
Related privileges	ItemSQLSelect, ItemTypeQuery, ItemQuery, ItemAdd, ItemSetUserAttr, ItemCheckInOut

ItemQuery

Users with this privilege can search items.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskMinimum, ClientTaskView
Required privileges	none
Related privileges	ItemSQLSelect, ItemTypeQuery

ItemRecordsAdmin

Users with this privilege can retrieve records, bypassing the IBM Records Manager record access control. This privilege does not allow users to update or delete records. For more information about records, see the *IBM DB2 Records Administrator's Guide*.

Used by	System administrators
Member of privilege sets	AllPrivs
Member of privilege groups	None
Required privileges	None
Related privileges	None

ItemRemoveLink

Users with this privilege can remove a link between two items, either in the same item type or in different item types.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemLinkTo, ItemLinked, ItemCheckInOut
Related privileges	ItemLinkTo, ItemLinked, ItemAddLink

ItemRoute

Users with this privilege can route a document from one work node to the next work node. This privilege is related to document routing.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemGetWorkList, ItemRouteEnd, ItemRouteStart, ItemUpdateWork

ItemRouteEnd

Users with this privilege can end a document routing process at any stage.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemGetWorkList, ItemRoute, ItemRouteStart, ItemUpdateWork

ItemRouteStart

Users with this privilege can start a document routing process.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemGetWorkList, ItemRoute, ItemRouteEnd, ItemUpdateWork

ItemSetACL

Users with this privilege can update the access control list of an item, if they have the ItemSetACL in their general privilege set and assigned to them in the existing ACL rule of the item being updated.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll
Required privileges	ItemCheckInOut
Related privileges	ItemSetUserAttr

ItemSetSysAttr

Users with this privilege can update system-defined attribute values of an item. The only system-defined attribute you can update are access control lists.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll
Required privileges	ItemCheckInOut
Related privileges	ItemCheckInOut, ItemSetUserAttr

ItemSetUserAttr

Users with this privilege can update user-defined attribute values of an item or document and modify the document parts.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	ItemCheckInOut
Related privileges	ItemAddPart, ItemUpdatePart, ItemRemovePart, ItemSetSysAttr, ItemSQLSelect, ItemTypeQuery, ItemQuery, ItemAdd, ItemDelete, ItemCheckInOut

ItemSQLSelect

Users with this privilege can retrieve items and the linked items and the resource parts for documents.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskMinimum, ClientTaskView
Required privileges	ItemQuery
Related privileges	ItemTypeQuery, ItemQuery

ItemSuperAccess

Users with this privilege can bypass the access control list checking, but not your assigned privileges.

Used by	Client users
----------------	--------------

Member of privilege sets	AllPrivs, ClientUserAllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll
Required privileges	none
Related privileges	none

ItemSuperCheckIn

Users with this privilege can check in or check out an item that was checked out by another user ID.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll
Required privileges	none
Related privileges	ItemCheckInOut

ItemTypeQuery

Users with this privilege can retrieve item type, component type, and related item type views.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskMinimum, ClientTaskView
Required privileges	none
Related privileges	ItemSQLSelect, ItemQuery, SystemDefineItemType

ItemUpdateWork

Users with this privilege can suspend, resume, and change priority of a work item. This privilege is related to document routing.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemGetWorkList, ItemRoute, ItemRouteEnd, ItemRouteStart

UserACLOwner

Users with this privilege can create User ACLs and also give ownership of a User ACL to a user. Ownership of a User ACL is given to users who have the UserACLOwner privilege in both their general privilege set and assigned to them in the User ACL rules.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll
Required privileges	none
Related privileges	ItemSetUserAttr

Document routing privileges:

These are the privileges related to document routing, with relevant access control list information.

ItemAdd

Users with this privilege can create items or documents. This privilege is also needed in order to define (or add) a document routing process definition to the system.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskCreate, ClientTaskUpdate
Required privileges	none
Related privileges	ItemTypeQuery, ItemSetUserAttr, ItemDelete, ItemAddPart, ItemRouteStart

ItemDelete

Users with this privilege can delete items and documents. This privilege is required to delete a document routing definition.

To delete an item and its associated parts, users need this privilege in their general privilege set and in the privilege set associated with the users in the access control list for the document and any associated parts.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskUpdate
Required privileges	none

Related privileges	ItemAdd, ItemSQLSelect, ItemTypeQuery, ItemQuery, ItemRemoveLink
---------------------------	--

ItemGetAssignedWork

Users with this privilege can retrieve work items assigned to another user. This privilege is related to work assignment in document routing.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll
Required privileges	none
Related privileges	ItemGetWork, ItemGetWorkList, ItemRoute, ItemRouteEnd, ItemRouteStart, ItemUpdateWork

ItemGetWorkList

Users with this privilege can retrieve work lists for document routing.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemRoute, ItemRouteEnd, ItemRouteStart, ItemUpdateWork

To retrieve a work list, the work list ACL is evaluated and the privilege required is ItemGetWorkList. If a user is trying to retrieve a work list that is assigned to another user, in addition to privilege ItemGetWorkList, the user needs to have ItemGetAssignedWork in the work list ACL.

When retrieving a work list, the user also needs to have access to the documents that belong to the work packages of that work list. Based on how the ACL of the document's item type is set, the user needs to be in the ACL of the document or of the document's item type with privilege ItemSQLSelect.

ItemGetWork

Users with this privilege can retrieve work packages for document routing.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, ClientUserReadOnly, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting

Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWorkList, ItemRoute, ItemRouteEnd, ItemRouteStart, ItemUpdateWork

To retrieve a particular work package from a work list, the work list ACL needs to include privilege ItemGetWork. If a user is trying to retrieve a work package that is assigned to another user, in addition to privilege ItemGetWork, the user needs to have ItemGetAssignedWork in the work list ACL.

Similar to retrieving a work list, the user also needs access to the work package's document. Based on how the ACL of the document's item type is set, the user needs to be in the ACL of the document or of the document's item type with privilegeItemSQLSelect. In the absence of this privilege, that particular work package is not returned.

ItemRoute

Users with this privilege can route a document from one work node to the next work node. This privilege is related to document routing.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemGetWorkList, ItemRouteEnd, ItemRouteStart, ItemUpdateWork

To route a work package to the next work node, the privilege required is ItemRoute. The ACL check is done at the current work node. Privilege ItemRoute is also checked when the work package is routed to the end node of the document routing process.

ItemRouteEnd

Users with this privilege can end a document routing process at any stage.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemGetWorkList, ItemRoute, ItemRouteStart, ItemUpdateWork

To end a process, the current work node ACL is evaluated and the privilege required is ItemRouteEnd. The ItemRouteEnd is checked when the process is explicitly ended.

ItemRouteStart

Users with this privilege can start a document routing process.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserCreateAndDelete, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemGetWorkList, ItemRoute, ItemRouteEnd, ItemUpdateWork

To start a new instance of a document routing process, the process ACL is evaluated and the privilege required is ItemRouteStart.

When routing a work package to a subprocess, the ACL of that subprocess is evaluated and the privilege required is ItemRouteStart.

ItemUpdateWork

Users with this privilege can suspend, resume, and change priority of a work item. This privilege is related to document routing.

Used by	Client users
Member of privilege sets	AllPrivs, ClientUserAllPrivs, ClientUserEdit, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	ClientTaskAll, ClientTaskDocRouting
Required privileges	none
Related privileges	ItemGetAssignedWork, ItemGetWork, ItemGetWorkList, ItemRoute, ItemRouteEnd, ItemRouteStart

To update the properties of a work package, that is to suspend, resume, change the priority, or change the user assigned to a work package, the work node ACL is evaluated and the privilege required is ItemUpdateWork.

Access control list checking

In the IBM Content Manager document routing processes, work lists and work nodes are managed like items. To create, delete, or update these document routing objects, you are required to have the following privileges: ItemAdd, ItemSetSysAttrs, ItemSetUserAttrs, or ItemDelete.

By default, an administrator user ID, with all privileges, is able to create, update, or delete document routing processes, work nodes, and work lists. However, an IBM Content Manager user ID that is not an administrator might not be able to perform such administrative tasks and might run into ACL check errors.

To allow users who do not have ItemSuperAccess privilege to create a new document routing process, work node, or work list, they must be added to the

DocRoutingACL, with a privilege set that contains ItemAdd. Also, users must have ItemAdd in their privilege set to create a new document routing object.

The ACL check for processes, work nodes, and work lists is at the item level. That is, each process instance, work node, or work list has its own ACL. To allow users who do not have ItemSuperAccess privilege to update or delete document routing administrative objects, they must be in the ACL of that particular object with a privilege set that contains the correct privileges.

To update an object, ItemSetSysAttrs and ItemSetUserAttrs must be in the associated privilege set. To delete an object, ItemDelete must be in the associated privilege set.

System privileges:

The privileges starting with *System* pertain to maintenance for all system administration functionality.

SystemBatchCompileACL

Users with this privilege can regenerate new and perform maintenance on access control list tables. You can also perform batch jobs offline.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerPrivsAndACL
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineACL, SystemSetACL

SystemDefineACL

Users with this privilege can create, update, and delete access control list definitions. You are also allowed to assign the access control list (ACL) to an existing administrative domain before the ACL can be used.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerPrivsAndACL
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemBatchCompileACL, SystemDefineACL

SystemDefineAttrs

With this privilege you can define, delete, and update attributes, attribute groups, and reference attributes.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerDataModel

Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineItemType

SystemDefineDomain

Users with this privilege can create, update, and delete administrative domain definitions.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerSubDomain
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemSuperDomainAdmin, SystemDomainAdmin, SystemDomainQuery, SystemDefineUser, SystemDefineRM, SystemDefinePrivs, SystemDefineACL, SystemDefineSMSColl, SystemQueryOtherDomains

SystemDefineGroup

Users with this privilege can create, update, and delete user groups and user group members.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerUsers
Super privilege or privileges associated	SystemDomainAdmin, SystemSuperDomainAdmin
Related privileges	SystemDefineUser, SystemQueryGroup, SystemDomainQuery, SystemSetACL

SystemDefineItemType

Users with this privilege can create, update name, and delete definitions of item types, component types, item type views, and component views.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerDataModel
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineAttrs, SystemDefineRM, SystemDefineSMSColl, SystemDefineACL, SystemDefineLinkType, SystemDefineMimeType, SystemDefineSemanticType, SystemDefineXdoObject

SystemDefineLinkType

Users with this privilege can create, update, and delete link type definitions.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminSuper
Member of privilege groups	AdministerDataModel
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineItemType

SystemDefineMimeType

Users with this privilege can create, update, and delete MIME types.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerDataModel
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineItemType

SystemDefineNewKywdClass

With this privilege you can create a new keyword classification in the keyword table.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerDataModel
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemQueryAllKywdClass, SystemDefineNLSTLang

SystemDefineNLSTLang

This privilege is used to define the NLS language used in all system administration objects.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerDataModel, AdministerRMServer
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineNewKywdClass, SystemQueryAllKywdClass

SystemDefinePrivs

Users with this privilege can create, update, and delete privileges, privilege groups, and privilege sets. You are also able to assign a privilege set to an administration domain.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerPrivsAndACL
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineUser, SystemGrantUserPrivs, SystemSetGrantPrivs, SystemQueryUserPrivs, SystemSetACL

SystemDefineRM

Users with this privilege can create, update, and delete resource manager definitions and resource manager access type definitions.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminSubDomainCM, SysAdminSuper
Member of privilege groups	AdministerRMServer
Super privilege or privileges associated	SystemDomainAdmin, SystemSuperDomainAdmin
Related privileges	SystemDefineXdoObject, SystemDefineSMSColl, SystemSetReplicaRule, SystemManageKey, SystemGetKey

SystemDefineSemanticType

Users with this privilege can create, update, and delete semantic type definitions.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminSuper
Member of privilege groups	AdministerDataModel
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineItemType

SystemDefineSMSColl

Users with this privilege can create, update, and delete SMS collections on the resource managers.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminSubDomainCM, SysAdminSuper
Member of privilege groups	AdministerRMServer

Super privilege or privileges associated	SystemDomainAdmin, SystemSuperDomainAdmin
Related privileges	SystemDefineRM, SystemSetReplicaRule

SystemDefineUser

Users with this privilege can create, update, and delete users.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerUsers
Super privilege or privileges associated	SystemDomainAdmin, SystemSuperDomainAdmin
Related privileges	SystemDomainQuery, SystemGrantUserPrivs, SystemSetGrantPrivs, SystemQueryUserPrivs, SystemDefineGroup, SystemQueryGroup, SystemDefineACL, SystemDefinePrivs, SystemSetACL

SystemDefineXdoObject

Users with this privilege can create, update, and delete XDO objects.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminSuper
Member of privilege groups	AdministerDataModel
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineItemType, SystemDefineRM

SystemDomainAdmin

Users with this privilege can administer an assigned sub-domain. You can also use the privilege set and access control lists assigned to the domain when creating users. SystemDomainAdmin lets you manager users, user groups, resource managers, and collections that belong to your domain.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminSubDomainCM, SysAdminSuper
Member of privilege groups	AdministerSubDomain
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemSuperDomainAdmin, SystemDomainQuery, SystemDefineUser, SystemDefineGroup, SystemQueryGroup, SystemDefineDomain, SystemDefineRM, SystemDefineSMSColl

SystemDomainQuery

With this privilege you are able to query all the system objects that have been assigned to your sub-domain. SystemDomainQuery allows you to see the objects (access control lists, privilege sets, resource managers, collections, users, and user groups) assigned to your sub-domain.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerSubDomain
Super privilege or privileges associated	SystemDomainAdmin, SystemSuperDomainAdmin
Related privileges	SystemSuperDomainAdmin, SystemDomainAdmin, SystemDefineUser, SystemDefineGroup, SystemDefineDomain, SystemDefineRM, SystemDefineSMSColl

SystemGetKey

Users with this privilege can retrieve encryption keys that allow you to talk to the resource manager.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminSubDomainCM, SysAdminSuper
Member of privilege groups	AdministerRMServer
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineRM, SystemManageKey

SystemGrantUserPrivs

Users with this privilege can grant privilege sets to a specified user. Without this privilege, the privilege set defined in your grant privilege set will be used for any new user created by you.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerUsers
Super privilege or privileges associated	SystemDomainAdmin, SystemSuperDomainAdmin
Related privileges	SystemSetGrantPrivs, SystemDefineUser, SystemQueryUserPrivs

SystemManageKey

Users with this privilege can manage (reset or replace) encryption keys that allow you to gain access to a specific object or objects stored on the resource manager.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminSubDomainCM, SysAdminSuper
Member of privilege groups	AdministerRMServer
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineRM, SystemGetKey

SystemQueryAllKywdClass

Users with this privilege can see all keyword classes and keyword codes, including the name and description, at one time.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerDataModel
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemDefineNewKywdClass, SystemDefineNLSLang

SystemQueryGroup

Users with this privilege can see user groups, including the group description and users in the group, in your administration domain. Unless you have access to the super domain you will only see the user groups in your sub-domain.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerUsers
Super privilege or privileges associated	SystemDomainQuery, SystemDomainAdmin, SystemSuperDomainAdmin
Related privileges	SystemDomainQuery, SystemDefineUser, SystemDefineGroup

SystemQueryOtherDomains

Users with this privilege can see users, user groups, resource managers, and collections in other sub-domains. Without the SystemQueryOtherDomains privilege you can only see these definitions in your sub-domain and the public domain.

Used by	System administrators
----------------	-----------------------

Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerSubDomain
Super privilege or privileges associated	SystemSuperDomainAdmin
Related privileges	SystemSuperDomainAdmin, SystemDomainAdmin, SystemDomainQuery, SystemDefineDomain

SystemQueryUserPrivs

Users with this privilege can see other user's information in your domain. When you are retrieving an ACL, this privilege also is required so that you can view the user's information along with the ACL.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerUsers
Super privilege or privileges associated	SystemDomainQuery, SystemDomainAdmin, SystemSuperDomainAdmin
Related privileges	SystemDomainQuery, SystemDefineUser, SystemQueryOtherDomains, SystemQueryGroup

SystemSetACL

This privilege is used to associate users with an access control list (ACL). In order to assign users and user groups to an ACL you must have this privilege.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerPrivsAndACL, AdministerUsers
Super privilege or privileges associated	SystemDomainAdmin, SystemSuperDomainAdmin
Related privileges	SystemBatchCompileACL, SystemDefineACL

SystemSetCtrlParm

Users with this privilege can set up the following configurations for the library server: trace level, trace file name, ACL binding, public access, library server ACL, default ACL choice for an item, system administration event, system administration domain, and DB2 Net Search Extender user.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	AdministerRMServer
Super privilege or privileges associated	SystemSuperDomainAdmin

Related privileges	SystemSuperDomainAdmin, SystemManageKey, SystemDefineNLSLang
---------------------------	---

SystemSetGrantPrivs

Users with this privilege can assign any grant privilege set to users you create. If you don't have this privilege, your grant privilege will automatically be assigned to any user you create.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSubDomainCM, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerUsers
Super privilege or privileges associated	none
Related privileges	SystemGrantUserPrivs

SystemSetReplicaRule

Users with this privilege can create replica rules for your backup resource manager or resource managers.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminSuper
Member of privilege groups	AdministerRMServer
Super privilege or privileges associated	SystemSuperDomainAdmin, SystemDomainAdmin
Related privileges	SystemDefineRM, SystemDefineSMSColl

SystemSuperDomainAdmin

Users with this privilege can perform all system administration functions such as define item type, users, access control lists, resource manager, and so forth.

Used by	System administrators
Member of privilege sets	AllPrivs, SysAdminCM, SysAdminEIP, SysAdminSuper
Member of privilege groups	none
Super privilege or privileges associated	none
Related privileges	All privileges above

WF privileges:

The privileges starting with *WF* pertain to using and administering advanced workflow in IBM Information Integrator for Content. These privileges do not apply to the document routing feature in IBM Content Manager.

WFSuperWorkFlowPriv

Allow super access to administer workflows. Users with this administrative control over IBM Content Manager workflow processes, including the ability to assign unclaimed work items to specific users and the ability to suspend, resume, or terminate workflows. The WFSuperWorkFlowPriv privilege does not automatically include the WFWorklist privilege.

Used by	Advanced workflow administrators
Member of privilege sets	AllPrivs, SysAdminEIP, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerWorkFlow
Required privileges	none
Related privileges	WFWorklist

WFWorklist

Add, update, delete, and retrieve worklists. Users with this privilege can participate in the workflow process and use workflow APIs that access and modify worklist data. This is the minimum privilege required to access workflow data.

Used by	Advanced workflow users
Member of privilege sets	AllPrivs, SysAdminEIP, SysAdminSubDomainEIP, SysAdminSuper
Member of privilege groups	AdministerWorkFlow
Required privileges	none
Related privileges	WFSuperWorkFlowPriv

Viewing or modifying privileges:

Restriction: You can modify only the description for a user-defined privilege. You cannot modify a system-defined privilege.

To view or modify a privilege, complete the following steps:

1. Expand **Authorization** in the navigation pane.
2. Click **Privileges** to display a list of privileges in the details pane.
3. Right-click a privilege in the right pane and click **Properties**. The Privilege Properties window opens where you can view or modify the privilege.
4. Click **OK** to save any changes that you made.

Copying privileges:

You can copy a privilege to simplify the task of creating a new privilege.

To copy a privilege:

1. Expand **Authorization** in the navigation pane.
2. Click **Privileges**. A list of privileges is displayed in the details pane.
3. Right-click a privilege and click **Copy**.
4. In the **Privilege name** field of the Copy Privilege window, type a new name for the privilege.

5. In the **Description** field, type a description that can help you identify the new privilege.
6. Click **OK** to save the privilege.

Deleting privileges:

Restrictions:

- You can modify or delete user-defined privileges; however, you cannot undo a deletion.
- You cannot modify or delete system-defined privileges.

To delete a privilege:

1. Expand **Authorization** in the navigation pane.
2. Click **Privileges** to display a list of privileges in the details pane.
3. Right-click the privilege that you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

Creating privilege sets

Restriction: If you enable administrative domains, you must belong to the SuperDomain, where you can manage system objects for all domains, to define access control lists or privilege sets. If you do not belong to the SuperDomain, you can define access control lists or privilege sets if you assign the privilege to create access control lists or privilege sets to a domain. Access control lists and privilege sets can associate with multiple domains, but they cannot be managed by users in any subdomains.

There are two ways that you can create a privilege set:

- “Creating a privilege set (basic)” on page 508
- “Creating a privilege set (advanced)” on page 508

In the basic creation, you can create a privilege set by selecting roles that have a description of what actions the role will allow. The advanced creation allows you to create all aspects of the privilege set including individual privileges.

Privilege sets:

A *privilege set* is a collection of privileges that are used to work with system components and functions.

A privilege set represents a user role, such as an editor or reviewer. The administrator assigns privilege sets to user IDs.

The system administration client has several system defined privilege sets that are already available by default. The predefined privilege sets provide for many of the common functions for which IBM Content Manager can be used. These privilege sets can also be copied to create similar privilege sets with expanded capabilities. Because the predefined privilege sets can be copied, you might be able to base any new privilege sets that you need to create on the existing predefined ones, instead of creating entirely new privilege sets.

To determine whether the predefined privilege sets can be copied to create any customized privilege sets that you need, you can view the descriptions of these sets in the right pane of the system administration client. To view the descriptions, expand **Authorization** in the system administration tree and click **Privilege Sets**.

Individual privileges or privilege groups can be put together to form a privilege set. A privilege set can be assigned to users directly, can be used to set up ACL rules, and can be associated with a domain.

Privilege sets take effect at privilege checking time.

Creating a privilege set (basic):

To create a privilege set using the basic creation, complete the following steps:

1. Expand **Authorization** in the tree view.
2. Right-click **Privilege Sets** and click **New > Basic**.
3. In the **Name** field, type a descriptive name for the privilege set that you are creating. For example, the name AdminPrivs might describe privileges associated with administrators.
4. Optional: In the **Description** field, type a description that will help you identify your new privilege set.
5. Select **Administrative privileges** if you want all administrative privileges or select the administrative privileges you want your users to have.
6. Select **Client privileges** if you want all client privileges or select the client privileges you want your users to have.
7. Click **OK** to save the new privilege set and close the window. Click **Apply** to save the privilege set and to leave the window open to define another privilege set.

Creating a privilege set (advanced):

To create a privilege set using the advanced creation, which grants specific access to see all privileges included on the IBM Content Manager system, complete the following steps:

1. Expand **Authorization** in the tree view.
2. Right-click **Privilege Sets** and click **New > Advanced**.
3. In the **Name** field, type a descriptive name for the privilege set that you are creating. For example, the name AdminPrivs might describe privileges associated with administrators.
4. Optional: In the **Description** field, type a description that will help you identify your new privilege set.
5. If administrative domains are enabled, select the target domain for this privilege set. The default domain, PublicDomain, allows any user from any domain who can create and assign privileges access to this privilege set.
6. Select a privilege group from the **Privilege groups** list to see the privileges within that group. If you want to see all available privileges, select **All** from the list. Use the search button below the list to find specific privilege groups.
7. Select one or more privileges from the **Privileges** list to belong to this privilege set. You can select all of the privileges in the list by selecting the **Select all** check box. Use the search button below the list to find specific privileges. Each privilege that you select moves to the **Selected privileges** list.
8. Optional: To remove any privilege from the **Selected privileges** list, select the privilege and click **Remove**.
9. Click **OK** to save the new privilege set and close the window. Click **Apply** to save the privilege set and to leave the window open to define another privilege set.

Predefined privilege sets:

The system provides several predefined privilege sets that define access rights for most users. Because of these predefined privilege sets, administrators have less need to define additional privilege sets. You can view descriptions of several predefined privilege sets in the right pane of the system administration client when you expand **Authorization** in the system administration tree and click **Privilege Sets**. Administrators can also create new privilege sets by modifying the existing privilege sets to suit their particular needs.

The following table lists the predefined privilege sets in IBM Content Manager and IBM Information Integrator for Content, and identifies the privileges that belong to each set.

Table 81. Predefined privilege sets

Privilege set	Privilege set definition	Privileges in set
AllPrivs	For a system administrator who can perform all of the tasks described under the other privileges, including all client privileges.	All privileges
ClientUserAllPrivs	For a user who can perform all client tasks, but does not have administrator privileges. The user can search documents and perform process and folder related actions.	All <i>Client</i> and <i>Item</i> privileges
ClientUserCreateAndDelete	For a user who can load documents into IBM Content Manager, import and scan items, index documents, and start items on workflow and delete items.	<ul style="list-style-type: none">ClientAddNewBasePart, ClientDeleteBasePart, ClientImport, ClientReadAnnotation, ClientReadBasePart, ClientScanItemAdd, ItemAddLink, ItemCheckInOut, ItemDelete, ItemLinked, ItemLinkTo, ItemQuery, ItemRemoveLink, ItemRouteStart, ItemSQLSelect, ItemTypeQuery
ClientUserEdit	For a user who can update items, annotations, and note logs, can perform searches, and can view and print documents.	<ul style="list-style-type: none">All <i>Client</i> privilegesItemAdd, ItemAddLink, ItemCheckInOut, ItemDelete, ItemGetWork, ItemGetWorkList, ItemLinked, ItemLinkTo, ItemMove, ItemQuery, ItemRemoveLink, ItemRoute, ItemRouteEnd, ItemRouteStart, ItemSetUserAttr, ItemSQLSelect, ItemTypeQuery, ItemUpdateWork
ClientUserReadOnly	For a user who can search, view, and print documents, and view annotations and note logs. The user cannot perform process related actions, folder related actions, or make any updates.	<ul style="list-style-type: none">ClientAdvancedSearch, ClientExport, ClientPrint, ClientReadAnnotation, ClientReadBasePart, ClientReadHistory, ClientReadNoteLogItemGetWork, ItemGetWorkList, ItemQuery, ItemSQLSelect, ItemTypeQuery

Table 81. Predefined privilege sets (continued)

Privilege set	Privilege set definition	Privileges in set
SysAdminCM	For an IBM Content Manager administrator who can perform all IBM Content Manager system administration tasks including managing users, privileges, and access control lists, administering the data model, and performing client tasks.	All <i>Client</i> , <i>Item</i> , and <i>System</i> privileges
SysAdminEIP	For an IBM Content Manager system administrator who can perform all IBM Content Manager system administration tasks including managing users, privileges, and access control lists, working with federated entities and domains, and performing all client tasks.	<ul style="list-style-type: none"> • All <i>Client</i>, <i>EIPAdmin</i>, <i>IKF</i>, <i>Item</i>, and <i>WF</i> privileges • SystemDefineGroup, SystemDefineUser, SystemDomainQuery, SystemGrantUserPrivs, SystemQueryAllKywdClass, SystemQueryGroup, SystemQueryUserPrivs, SystemSetACL, SystemSetGrantPrivs
SysAdminSubDomainCM	For a system administrator who can work only with subdomains and users, groups, privilege sets, access control lists, and resource managers. Includes all client tasks.	<ul style="list-style-type: none"> • All <i>Client</i> privileges • ItemAdd, ItemAddLink, ItemCheckInOut, ItemDelete, ItemGetAssignedWork, ItemGetWork, ItemGetWorkList, ItemLinked, ItemLinkTo, ItemMove, ItemQuery, ItemRemoveLink, ItemRoute, ItemRouteEnd, ItemRouteStart, ItemSetSysAttr, ItemSetUserAttr, ItemSQLSelect, ItemSuperCheckInOut, ItemTypeQuery, ItemUpdateWork • SystemDefineGroup, SystemDefineRM, SystemDefineSMSColl, SystemDefineUser, SystemDomainAdmin, SystemDomainQuery, SystemGetKey, SystemGrantUserPrivs, SystemManageKey, SystemQueryAllKywdClass, SystemQueryGroup, SystemQueryUserPrivs, SystemSetACL, SystemSetGrantPrivs
SysAdminSubDomainEIP	For an IBM Content Manager system administrator who can work only with subdomains and users, groups, privilege sets, and access control lists. Includes all client tasks.	<ul style="list-style-type: none"> • All <i>Client</i>, <i>EIPAdmin</i>, <i>IKF</i>, <i>Item</i>, and <i>WF</i> privileges • SystemDefineGroup, SystemDefineUser, SystemDomainQuery, SystemGrantUserPrivs, SystemQueryAllKywdClass, SystemQueryGroup, SystemQueryUserPrivs, SystemSetACL, SystemSetGrantPrivs
SysAdminSuper	For a system administrator who can perform all Content Manager and Information Integrator for Content system administration tasks, and all client tasks.	All <i>Client</i> , <i>EIPAdmin</i> , <i>IKF</i> , <i>Item</i> , <i>WF</i> and <i>System</i> privileges
UserDBConnect	Allows users to connect to the database without having their own database user ID. The users are required to enter a password.	AllowConnectToLogon

Table 81. Predefined privilege sets (continued)

Privilege set	Privilege set definition	Privileges in set
UserDBTrustedConnect	Allows users to connect to the database without having their own database user ID. The users do not have to enter a password.	AllowConnectToLogon, AllowTrustedLogon
Noprivs	No privileges at all. This might be useful for a temporary user setting.	None

Viewing or modifying privilege sets (basic):

As your system progresses and changes, you also need to address the changing needs of user access. Regularly evaluate the access needs of your users. They need the appropriate access to objects to accomplish their jobs. You might even need to restrict their access.

To view or modify a basic privilege set, complete the following steps:

1. Expand **Authorization** in the tree view.
2. Right-click **Privilege Sets** and click **New > Basic**.
3. Optional: In the **Description** field, modify the description that will help you identify your privilege set.
4. Select **Administrative privileges** if you want all administrative privileges or select the administrative privileges you want your users to have.
5. Select **Client privileges** if you want all client privileges or select the client privileges you want your users to have.
6. Click **OK** to save the new privilege set and close the window. Click **Apply** to save the privilege set and to leave the window open to define another privilege set.

Viewing or modifying privilege sets (advanced):

As your system progresses and changes, you also need to address the changing needs of user access. Regularly evaluate the access needs of your users. They need the appropriate access to objects to accomplish their jobs. You might even need to restrict their access.

To view or modify an advanced privilege set, complete the following steps:

1. Expand **Authorization** in the tree view.
2. Click **Privilege Sets** to display a list of privilege sets in the right pane.
3. Right-click a privilege set and click **Properties > Advanced**. The Properties window opens. The name of the privilege set is displayed. You cannot change it.
4. Optional: In the **Description** field, type a description to help identify the privilege set.
5. If administrative domains are enabled, select the target domain for this privilege set. The default domain, **PublicDomain**, allows any user from any domain who can create and assign privileges to access this privilege set.
6. Select a privilege group from the **Privilege groups** list. If you want to see all available privileges, select **All** from the list. Use the search field below the list box to find specific privilege groups.

7. Select one or more privileges from the **Privileges** list to belong to this privilege set. You can select all of the privileges in the privilege group by selecting the **Select all** check box. Use the search button below the list to find specific privileges. Each privilege that you select moves to the **Selected privileges** list.
8. Optional: To remove any privilege from the **Selected privileges** list, select the privilege and click **Remove**.
9. Click **OK** to save any changes you made to the privilege set and close the window. Click **Apply** to save the privilege set and to leave the window open to make any further modifications.

Copying privilege sets (basic):

To copy a basic privilege set, complete the following steps:

Note: When copying a privilege set the only field that must change is the Name field. All other fields will be populated with the information from the privilege set that was copied. Modifying those fields is optional.

1. Expand **Authorization** in the tree view.
2. Right-click **Privilege Sets** and click **New > Basic**.
3. In the **Name** field, type a descriptive name for the privilege set that you are creating. For example, the name AdminPrivs might describe privileges associated with administrators.
4. Optional: In the **Description** field, type a description that will help you identify your new privilege set.
5. Select Administrative privileges if you want all administrative privileges or select the administrative privileges you want your users to have.
6. Select Client privileges if you want all client privileges or select the client privileges you want your users to have.
7. Click **OK** to save the new privilege set and close the window. Click **Apply** to save the privilege set and to leave the window open to define another privilege set.

Copying privilege sets (advanced):

To copy an advanced privilege set, complete the following steps:

Note: When copying a privilege set the only field that must change is the Name field. All other fields will be populated with the information from the privilege set that was copied. Modifying those fields is optional.

1. Expand **Authorization** in the navigation pane.
2. Click **Privilege Sets** to display a list of privilege sets in the details pane.
3. Right-click a privilege set and click **Copy > Advanced** to open the Copy window.
4. In the **Name** field, rename the privilege set with a descriptive name. For example, the name AdminPrivs might describe privileges associated with administrators.
5. Optional: In the **Description** field, type a description to help identify the privilege set.
6. Optional: If administrative domains are enabled, select the target domain for this privilege set. The default domain, PublicDomain, allows any user from any domain who can create and assign privileges access to this privilege set.

7. Optional: If you do not want an exact copy, select a privilege group from the **Privilege groups** list. If you want to see all available privileges, select **All** from the list. Use the search button below the list to find specific privilege groups.
8. Optional: Select one or more privileges from the **Privileges** list to belong to this privilege set. You can select all of the privileges in the privilege group by selecting the **Select all** check box. Use the search button below the list to find specific privileges. Each privilege that you select moves to the **Selected privileges** list.
9. Optional: To remove any privilege from the **Selected privileges** list box, select the privilege and click **Remove**.
10. Click **OK** to save the privilege set and close the window. Click **Apply** to save the privilege set and to leave the window open to define another privilege set.

Deleting privilege sets:

Note: Some system defined privilege sets cannot be deleted. If you are not allowed to delete the privilege set because it is a system defined privilege set or it is in use, you will get a warning.

To delete a privilege set:

1. Expand **Authorization** in the tree view.
2. Click **Privilege Sets** to display a list of privilege sets in the details pane.
3. Right-click the privilege set that you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

Assigning a privilege set to an access control list:

Each user ID or user group that you add to an access control list (ACL) must have a privilege set associated with it.

The user ID or user group and privilege set define which users have access to an object and what type of access they have to that object.

Users cannot access any object unless they are on the appropriate ACL. To add a user or user group to an ACL in the New Access Control List Definition window, you select a user ID and a privilege set for the ACL and click **Add**. For each defined ACL, you can find the user IDs and groups listed in the Access Control List window. You can modify this table by adding and removing user IDs and groups.

Creating privilege groups

Before you create a privilege group, check the predefined privilege groups to see if they fulfill your needs or to see how they group privileges.

To create a privilege group:

1. Expand **Authorization** in the tree pane.
2. Right-click **Privilege Groups** and select **New**. The New Privilege Group window opens.
3. In the **Name** field, type a descriptive name for the privilege group that you are creating.
4. Optional: In the **Description** field, type a description that will help you identify the new privilege group.

5. Select one or more privileges from the **Available privileges** list. Use the search field below the list to find a specific privilege.
6. Click **Add** to add privileges to the **Selected privileges** list.
7. Optional: To remove privileges from the privilege group, select the privileges from the **Selected privileges** list and click **Remove**.
8. Click **OK** to save the new privilege group and close the window. Click **Apply** to save the privilege group and to leave the window open to define another privilege group.

Privilege groups: Privileges can be grouped together based on their demands, functions, user roles, and so forth. For example, creating users and deleting objects are privileges usually associated with system administration. You could put them in a privilege group called Administration for easy access when working with users and domains.

Privilege groups also allow you to quickly access the privileges that you want when you are creating privilege sets. When you create a privilege set for a system administrator, you can select the Administration privilege group to display those privileges. From that list, you can select the privileges that you want to include in the privilege set. By grouping privileges in privilege groups, you narrow your search from all privileges to a meaningful subset of them. It is also convenient to group privileges of custom applications that use their own set of privileges.

Note: Privilege groups are not taken into account when checking privileges.

Privilege group members:

The following table lists the predefined privilege groups in IBM Content Manager and IBM Information Integrator for Content, and identifies the privileges that belong to each group.

Table 82. Predefined privilege groups

Privilege group	Privileges in group
AdministerDataModel	SystemDefineAttrs, SystemDefineItemType, SystemDefineLinkType, SystemDefineMimeType, SystemDefineNewKywdClass, SystemDefineNLSLang, SystemDefineSemanticType, SystemDefineXdoObject, SystemQueryAllKywdClass
AdministerEIP	all <i>EIPAdmin</i> privileges
AdministerPrivsAndACL	SystemBatchCompileACL, SystemDefineACL, SystemDefinePrivs, SystemSetACL
AdministerRMServer	SystemDefineNLSLang, SystemDefineRM, SystemDefineSMSColl, SystemGetKey, SystemManageKey, SystemSetCtrlParm, SystemSetReplicaRule
AdministerSubDomain	SystemDefineDomain, SystemDomainAdmin, SystemDomainQuery, SystemQueryOtherDomains
AdministerUsers	SystemDefineGroup, SystemDefineUser, SystemGrantUserPrivs, SystemQueryGroup, SystemQueryUserPrivs, SystemSetACL, SystemSetGrantPrivs
AdministerWorkFlow	all <i>WF</i> privileges
ClientTaskAll	all <i>Client</i> and <i>Item</i> privileges

Table 82. Predefined privilege groups (continued)

Privilege group	Privileges in group
ClientTaskCreate	<ul style="list-style-type: none"> ClientAddNewBasePart, ClientImport, ClientScan ItemAdd, ItemCheckInOut
ClientTaskDocRouting	ItemGetWork, ItemGetWorkList, ItemRoute, ItemRouteEnd, ItemRouteStart, ItemUpdateWork
ClientTaskLogon	all <i>Allow</i> privileges
ClientTaskMinimum	<ul style="list-style-type: none"> ClientAdvancedSearch ItemQuery, ItemSQLSelect, ItemTypeQuery
ClientTaskUpdate	<ul style="list-style-type: none"> ClientAddNewBasePart, ClientAddToNoteLog, ClientDeleteBasePart, ClientModifyAnnotation, ClientModifyBasePart, ClientModifyNoteLog ItemAdd, ItemAddLink, ItemCheckInOut, ItemDelete, ItemLinked, ItemLinkTo, ItemMove, ItemRemoveLink, ItemSetUserAttr
ClientTaskView	<ul style="list-style-type: none"> ClientPrint, ClientReadAnnotation, ClientReadBasePart, ClientReadHistory, ClientReadNoteLog ItemQuery, ItemSQLSelect, ItemTypeQuery
IMDefineTaxonomy	IKFCreateCatalog, IKFCreateCategory, IKFDeleteCatalog, IKFDeleteCategory, IKFRetrieveCatalog, IKFRetrieveCategory, IKFUpdateCatalog, IKFUpdateCategory
IMImportDocs	IKFCreateRecord, IKFDeleteRecord, IKFRetrieveCatalog, IKFRetrieveCategory, IKFRetrieveRecord, IKFRunAnalysisFunc, IKFRunServerTask, IKFUpdateRecord
IMRetrieveDocs	IKFRetrieveCatalog, IKFRetrieveCategory, IKFRetrieveRecord, IKFRunServerTask
IMTrainDocuments	IKFCreateTrainingDoc, IKFDeleteTrainingDoc, IKFRetrieveCatalog, IKFRetrieveCategory, IKFRetrieveTrainingDoc, IKFRunAnalysisFunc, IKFRunServerTask, IKFUpdateCatalog, IKFUpdateTrainingDoc

Viewing or modifying privilege groups:

You can view, but cannot modify, the privilege groups that came with the product. You can change any privilege groups that you created.

To view or modify a privilege group:

1. Expand **Authorization** in the navigation pane.
2. Click **Privilege Groups** to display a list of privilege groups in the details pane.
3. Right-click a privilege group and click **Properties**. The Privilege Group Properties window opens. The name of the privilege group is displayed. You cannot change it.
4. Optional: In the **Description** field, type a description that will help you identify the privilege group.
5. Select one or more privileges from the **Available privileges** list. Use the search button below the list to find a specific privilege.
6. Click **Add** to add privileges to the **Selected privileges** list.

7. Optional: To remove privileges from the privilege group, select the privileges from the **Selected privileges** list and click **Remove**.
8. Click **OK** to save any changes you made to the privilege group and close the window. Click **Apply** to save any changes to the privilege group and to leave the window open to make further changes.

Copying privilege groups:

You can copy any of the provided privilege groups or ones that you created previously. To copy a privilege group:

1. Expand **Authorization** in the navigation pane.
2. Click **Privilege Groups** to display a list of privilege groups in the details pane.
3. Right-click a privilege group and click **Copy** to open the Properties window.
4. In the **Name** field, type a new name for the privilege group.
5. Optional: In the **Description** field, type a description that will help you identify the privilege group.
6. Select one or more privileges from the **Available privileges** list. Use the search field below the list to find a specific privilege.
7. Click **Add** to add privileges to the **Selected privileges** list.
8. Optional: To remove privileges from the privilege group, select the privileges from the **Selected privileges** list and click **Remove**.
9. Click **OK** to save the privilege group and close the window. Click **Apply** to save the privilege group and to leave the window open to define another privilege group.

Deleting privilege groups:

To delete a privilege group:

1. Expand **Authorization** in the navigation pane.
2. Click **Privilege Groups** to display a list of privilege groups in the details pane.
3. Right-click the privilege group that you want to delete and click **Delete**.
4. Click **OK** to confirm the deletion.

Administering users

You can use administrative domains to create divisions of the library server exclusive to a group of users.

Enabling administrative domains

Restrictions:

- After you enable administrative domains, you cannot disable them.
- If you enable administrative domains, you must belong to the SuperDomain, where you can manage system objects for all domains, to define access control lists or privilege sets. If you do not belong to the SuperDomain, you can define access control lists or privilege sets if you assign the privilege to create access control lists or privilege sets to a domain. Access control lists and privilege sets can associate with multiple domains, but they cannot be managed by users in any subdomains.
- Administrative domains are common across both the IBM Content Manager and IBM Information Integrator for Content system administration databases if they

share the same database. If you have both products installed, and if IBM Content Manager and IBM Information Integrator for Content do not share a common database, you can enable administrative domains on one database and not the other.

To enable administrative domains:

1. Click **Tools > Administrative Domains** to open the Administrative Domain window.
2. Select **Enable Administrative Domains**.
3. Click **OK** to save the information and close the window.
4. Restart the system administration client for the change to take effect.

Creating administrative domains

Restrictions:

- After you enable administrative domains, you cannot disable them.
- The three default domains (SuperDomain, PublicDomain, and DefaultDomain) cannot be modified, copied, or deleted.
- None of the objects in the system domain can be moved into any other domain.
- The system defined group name, ICMPUBLIC, cannot be moved out of the public domain.
- User IDs are never in the public domain because users cannot be shared.
- If you enable administrative domains, you must belong to the SuperDomain, where you can manage system objects for all domains, to define access control lists or privilege sets. If you do not belong to the SuperDomain, you can define access control lists or privilege sets if you assign the privilege to create access control lists or privilege sets to a domain. Access control lists and privilege sets can associate with multiple domains, but they cannot be managed by users in any subdomains.
- Administrative domains are common across both the IBM Content Manager and IBM Information Integrator for Content system administration databases if they share the same database. If you have both products installed, and if IBM Content Manager and IBM Information Integrator for Content do not share a common database, you can enable administrative domains on one database and not the other.

To create an administrative domain:

1. Expand your library server in the navigation pane.
2. Right-click **Administrative Domains** and click **New** to open the New Domain window.
3. On the Definition page, enter a name for the new domain in the **Name** field.
4. In the **Description** field, enter a description for the new domain.
5. Click **OK** to save the information.

Administrative domains

An administrative domain is a section of a library server that one or more administrators manage. The purpose of administrative domains is to limit administrative and user access to a section of the library server. Domains are not visible to users, so what you name your domains will only have meaning to you and the system administrators who manage them. Users do not know that you have limited them to a part of the system, meaning that they only know about items within that domain.

Domains limit both administrative and user access. An administrator with full privileges, a superadministrator, can delegate limited administrative privileges to another administrator and has access to all domains. They can create an object and assign it to a domain.

An administrator with limited privileges, a subadministrator, has access to only a section of the system. Subadministrators cannot change the domain of an object. They can, however, access the contents of their own domain and list or retrieve any object in the PUBLIC, or shared, domain.

Each domain can be assigned one or more administrators that manage user access within that domain, although it can be the same administrator for all domains. Only superadministrators can create ACLs that subadministrators can use to either add or delete user IDs and user groups. Subadministrators cannot create, update, or delete ACLs.

Administrative domains consist of user IDs, user groups, privilege sets, and access control lists. For IBM Content Manager, they also consist of resource managers and collections. User IDs, user groups, resource managers, and collections can only exist in one domain at a time. Privilege sets and access control lists can exist in more than one domain at a time.

You might consider using administrative domains if you have a large user base divided among many departments or you manage the library server for more than one company. For example, XYZ Insurance might want to divide the company by department because users in the Claims department do not need to view or work with any documents in the Sales department.

Remember:

- After you enable administrative domains, you cannot disable them.
- You must restart the system administration client to see the effect of enabling the administrative domains.
- Resource managers, collections, user IDs, and user groups can exist in only one domain at a time.
- Privilege sets and access control lists can exist in more than one domain at a time.
- Except for the PUBLIC (shared) domain, domains do not overlap.
- Any object created in the super administrative domain cannot be moved, whether if it is system generated or user created.

Viewing or modifying administrative domains

After you create a domain, you can modify only the description.

Restriction:

1. You cannot modify a system-defined administrative domain.
2. You will only be able to view domains if they are enabled.

To view or modify an administrative domain:

1. Expand your library server in the navigation pane.
2. Click **Administrative Domains** to display the existing domains in the details pane.

3. Right-click the domain you want to change and click **Properties** to open the Properties window. The administrative domain name is displayed. You cannot change it.
4. Optional: In the **Description** field, enter a description for the domain.
5. Click **OK** to save the information.

Copying administrative domains

You can copy an administrative domain to simplify the task of creating a new administrative domain.

Restriction: You cannot copy a system-defined administrative domain.

To copy an administrative domain:

1. Expand your library server in the navigation pane.
2. Click **Administrative Domains** to display the existing domains in the details pane.
3. Right-click the domain that you want to copy and click **Copy** to open the Copy window.
4. On the Definition page, enter a name for the new domain in the **Name** field.
5. Optional: In the **Description** field, enter a description for the domain.
6. Click **OK** to save the information.

Deleting administrative domains

You might need to delete an administrative domain as part of regular maintenance of your content management system.

Restriction:

- You cannot delete a system-defined administrative domain.
- You must empty all of the objects out of a domain before you can delete the domain. For example, if a particular user is still in a domain that you want to delete, you must go to the Properties window for that user. Then you must remove the user from the domain that you want to delete. When that step is complete, you can delete the domain.

To delete an administrative domain:

1. Expand your library server in the navigation pane.
2. Click **Administrative Domains** to display the existing domains in the details pane.
3. Right-click an existing domain and click **Properties** to open the Properties window and view the objects that exist in the domain.
4. Remove each of the objects from the domain. Open the Properties windows for those objects and remove the association between the object and that domain by changing the domain in the **Domain** list.
5. Right-click the domain that you want to delete and click **Delete**.
6. Click **OK** to confirm the deletion.

Assigning components to domains

When creating users, user groups, privilege sets, and collections you are able to assign these components to domains. You are also able to assign resource managers to domains.

- “Assigning a user to a domain” on page 520

- “Assigning a user group to a domain”
- “Assigning a collection to a domain”
- “Assigning a resource manager to a domain”

Assigning a user to a domain

When you create a user ID, you have the choice to assign it to a domain, or leave it in the default domain. You can change the domain of the user ID at a later time through the user properties.

A user ID can belong to only one domain at a time. You cannot assign a user to the shared domain (PUBLIC domain) because a user ID can never be shared.

Only superadministrators have the authority to create domains and assign users to those domains. A domain can have more than one subadministrator, but only the superadministrator can define who those administrators are by giving them system administration privileges within a privilege set.

Assigning a user group to a domain

Assigning a user group to a domain changes the domain designated for each user ID in that user group. A user ID can belong to only one domain at a time. It cannot be assigned to the shared domain (PUBLIC domain) because a user ID can never be shared. Any user ID included in a group that you assign is also moved to the new domain.

A user group name can belong to only one domain at a time. It can be assigned to the shared PUBLIC domain since user groups can be shared among different domains.

Assigning a collection to a domain

You can restrict user access to a certain collection on a resource manager by assigning it to a specific domain. If the resource manager is in the PUBLIC domain, you can assign a collection to any other defined domain. If the resource manager, however, is defined to a specific domain already, then you cannot assign the collection to another domain, even if you want to assign the collection to the PUBLIC domain.

A user needs access to the resource manager to access the collections on it, so you cannot restrict access to the resource manager without imposing the same restrictions to the collections on it.

Assigning a resource manager to a domain

You can restrict user access to certain resource managers by assigning them to a specific domain. When you define a new resource manager for an IBM Content Manager library server or IBM Information Integrator for Content administration database to access, you have the option to select a domain.

The default for all resource managers is PUBLIC. If you do not want everyone to have access to the resource manager, you need to assign it to a domain. If you do not see a domain that you can assign the resource manager to, you can still define the resource manager and then create the domain you need. After you have the appropriate domain defined, open the resource manager properties and select the domain.

Moving components from one domain to another

From time to time you might find the need to move components from one domain to another. Some components can be assigned to more than one domain. In this case, you might find the need to add or remove that component from certain domains.

- “Moving a user from one domain to another”
- “Moving a user group from one domain to another” on page 522
- “Moving a collection from one domain to another” on page 522
- “Moving a resource manager from one domain to another” on page 522
- “Moving an access control list from one domain to another” on page 522
- “Moving a privilege set from one domain to another” on page 523

Moving a user from one domain to another

You might find reason to remove certain users from one domain and add them to another.

The task of moving a user from one domain to another includes a step to find all the user groups that a user belongs to. Consider using the **Description** field in the User definition window as a way to remember which user groups a user is grouped in. The use of this field might make this task a little easier.

Important: This task is time consuming. If you do not perform the steps in this task carefully, the user for which you are making these changes can have problems with accessing the system.

Requirement: You must be a superadministrator to change the domain of a user.

Remember:

- At no time can a user be in the PUBLIC domain.
- Users cannot be shared.

To move a user from one domain to another:

1. Find all of the groups to which the user belongs.
2. For all of the groups to which the user belongs, do one of the following steps:
 - Move these groups to the PUBLIC domain.
 - Remove the user from all of the groups.
3. Move any resource managers associated with this user to the PUBLIC domain. Then move the collections for these resource managers to the target domain by opening the collection properties and selecting the target domain.
4. Open the properties of all privilege sets associated with the user in the target domain. If the privilege sets are not already in the target domain, you can change the domain by right-clicking on the privilege set and selecting **Properties > Advanced**. Select the new domain you want the user to belong to from the Administrative domain list.
5. Open the properties of access control lists associated with the user in the target domain. If the access control lists are not already in the target domain, you can change the domain by right-clicking on the access control list and selecting **Properties**. Select the new domain you want the user to belong to from the Administrative domain list.
6. Move the user to the target domain by opening the user properties and changing the user domain.

7. Optional: You can move the groups and resource manager that you moved in steps 2 and 3 from the PUBLIC domain to the target domain if there are no more users remaining in the source domain who are associated with the groups and resource managers that you moved. Otherwise, the groups and resource managers must stay in the PUBLIC domain to allow sharing for users in different domains.

Moving a user group from one domain to another

Important: This task can result in problems with accessing the system if you do not do it right.

Requirement: You must be a superadministrator to change the domain of a user group.

- If the user group is empty, delete the group from its current domain, then re-create the group and assign it to the target domain.
- If the user group is not empty, follow these steps:
 1. Identify all of the users that belong to this group.
 2. Delete the group from its current domain.
 3. Recreate the group and assign it to the target domain.
 4. Add all of the users to this newly created group.

Moving a collection from one domain to another

Requirement: You must be a superadministrator to change the domain of a collection.

Follow these steps to move a collection from one domain to another:

1. Identify the resource manager the collection belongs to.
2. Move the associated resource manager to the PUBLIC domain.
3. Move the collection to the target domain by opening the collection properties and selecting the target domain.
4. Move the resource manager to the target domain by opening the collection properties and selecting the target domain.

Moving a resource manager from one domain to another

You must be a superadministrator to change the domain of a resource manager. To move a resource manager to another domain, follow these steps:

- If the resource manager contains no collections, move the resource manager to the target domain by opening its properties and changing the domain to the target domain.
- If the resource manager contains collections, follow these steps:
 1. Move the resource manager to the PUBLIC domain.
 2. Move the collections to the target domain by opening the collection properties and selecting the target domain.
 3. Move the resource manager to the target domain by opening the collection properties and selecting the target domain.

Moving an access control list from one domain to another

Because access control lists can reside in multiple domains, you can add them to the target domain without moving them.

To select a different domain for an access control list (ACL):

1. Select the ACL that you want to modify.
2. Right-click the ACL and select **Properties**.
3. Select the new domain you want the ACL to belong to from the Administrative domain list.

Moving a privilege set from one domain to another

Because privilege sets can reside in multiple domains, you can add them to the target domain without moving them.

To select a different domain for a privilege set:

1. Select the privilege set that you want to modify.
2. Right-click the privilege set and select **Properties > Advanced**.
3. Select the new domain you want the privilege set to belong to from the Administrative domain list.

Managing advanced workflow with IBM Information Integrator for Content

Most business operations can be characterized as a set of interrelated processes. Work flows from one employee to another, and from one department to another. Some simple processes might require only a few steps, while more complex processes involve a number of employees in different departments.

IBM Information Integrator for Content advanced workflow is a work management tool that you use to direct work through a process to from one user to another. Users complete the work and make decisions throughout the process. For example, XYZ Insurance receives large volumes of claims forms in the mail. During the verification process, insurance claims adjusters need to gather documents such as photographs, appraisals, and expert reports. Employees spend several hours each day opening, sorting, filing, and monitoring information, as well as collecting pertinent documents for final approval.

This information moves from one employee to another as the information is received and checked. As the claim is completed, it might be handled by employees in more than one department.

End to end, deploying advanced workflow consists of three high-level tasks:

1. Plan a workflow process
2. Create a workflow process
3. Route documents (client users)

These three high-level tasks contain the following specific tasks:

Plan a workflow process

The following illustration shows the overall task flow for workflow, with the planning tasks expanded. These tasks are not described, but this graphic is provided for reference.

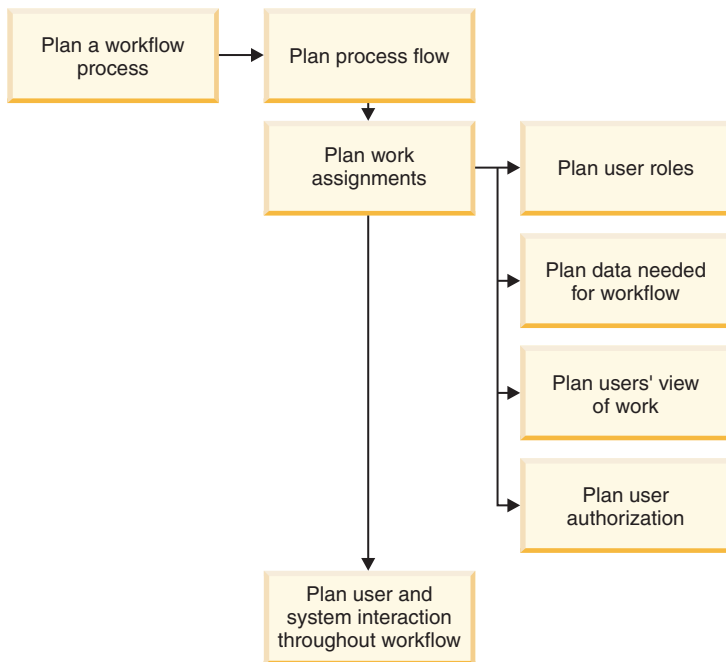


Figure 28. Common tasks for planning a workflow process

Create a workflow process

The following illustration shows the overall task flow for workflow, with the creation tasks expanded. These tasks are thoroughly described in this information.

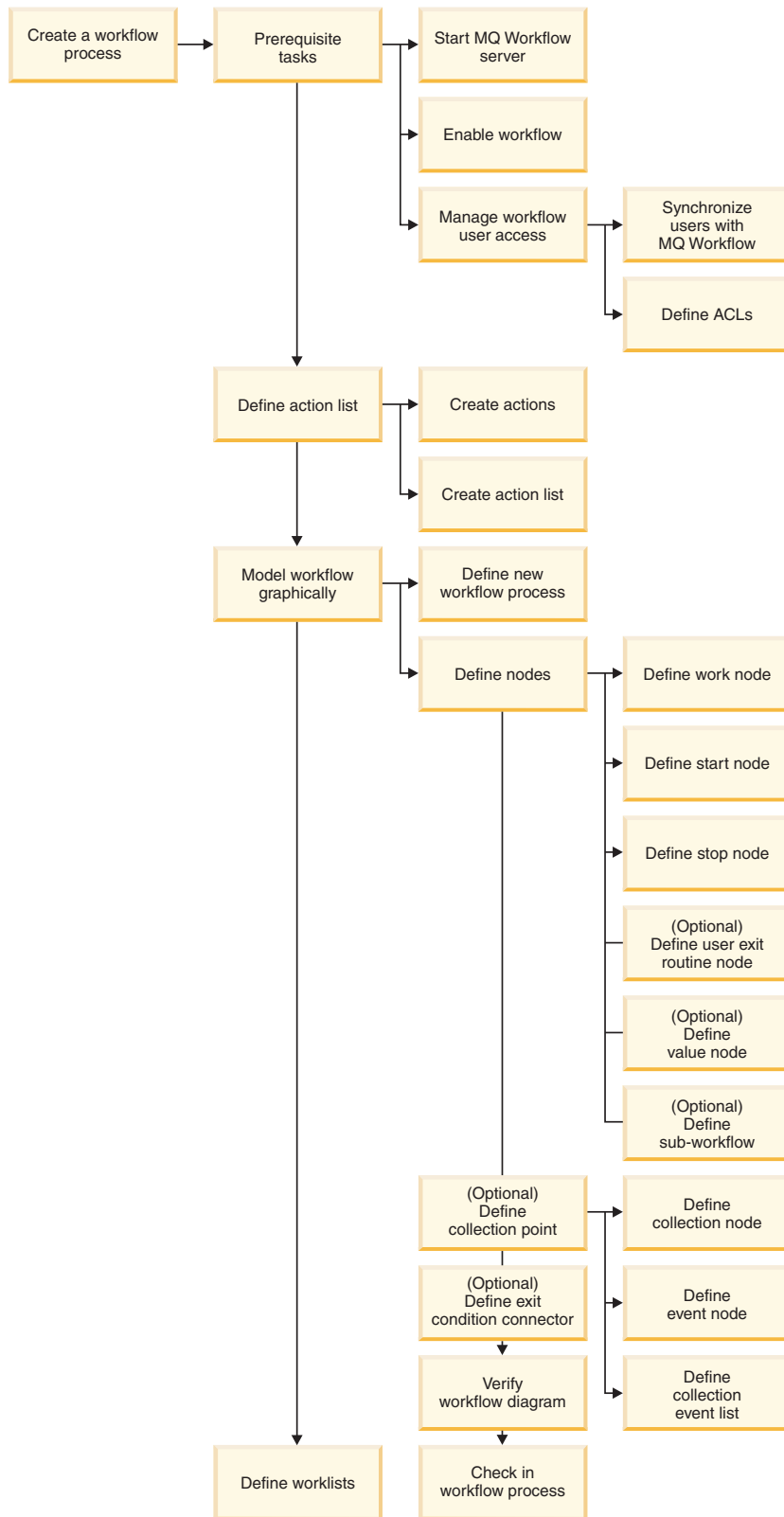


Figure 29. Common tasks for creating a workflow process

Route documents (client users)

These tasks are described in the eClient help.

Enterprise Information Portal Version 7.1 workflow users: IBM Content Manager does not provide any automated migration of Version 7.1 advanced workflow data. You must first redraw your Version 7.1 workflow diagrams using the IBM Content Manager advanced workflow builder and then redeploy those workflow processes.

You can also use IBM WebSphere Application Server (or IBM WebSphere Business Integration Server Foundation) Process Choreographer to perform workflow. See *Planning and Installing Your Content Management System* for more information.

“Creating a workflow process”

Related reference

“Comparison of IBM Content Manager workflow solutions” on page 249

Creating a workflow process

You complete most of the work to create a workflow inside of the graphical workflow builder. As summarized in the task list, before you can begin using workflow functionality, you must complete prerequisite tasks to start and enable workflow services and set up the necessary access control. Your users interact with the workflow process from the clients. You must specify the actions they can take on the work during the process and the worklist that they use to access the work on the process.

1. “Prerequisite tasks”
2. “Defining an action list” on page 532
3. “Modeling the workflow graphically” on page 537
4. “Defining a worklist” on page 559

Prerequisite tasks

Before you can create a workflow process, you must complete these tasks: start the IBM WebSphere MQ Workflow server, enable workflow services (if they were not previously enabled), and manage workflow user access.

1. “Starting the MQ Workflow server”
2. “Enabling workflow” on page 529
3. “Managing workflow user access” on page 529

Starting the MQ Workflow server

If you plan to use workflow functionality, you must start the MQ Workflow server before you launch the system administration client.

1. If you have not already done so, configure the MQ Workflow server for IBM Information Integrator for Content. See the information about installing and configuring IBM Information Integrator for Content in the planning and installing guide for details about configuring MQ Workflow server for use with IBM Information Integrator for Content.
2. On the machine where you installed MQ Workflow, start the MQ Workflow server by entering `cmbwfstart` at a command prompt. On Windows, two windows open for the MQ Workflow server. Leave the command windows open to continue running the server.
On UNIX systems, MQ Workflow runs as a background process.
3. Enable workflow if you have not previously enabled it.

Related concepts

Installing and configuring IBM Information Integrator for Content

Related reference

"Cannot start MQ Workflow server with cmbwfstart command" on page 676

Enabling workflow

Before you can use the advanced workflow functionality, you must start the workflow service.

1. Log in to the system administration client.
2. If you have multiple system administration databases, in the tree view, select the database where you want to enable workflow.
3. From the System Administration Client window, click **Tools > Services**. The Services window opens.
4. Select **Workflow**.
5. Click **OK**.
6. Log off from the system administration client and log in again.

If you have multiple databases, expand the icon for the database where you enabled advanced workflow. If you have the authority to administer workflow, the **Workflows** folder icon displays in the tree view below the database icon.

Workflow services remain enabled from session to session until you disable them.

Restriction: There is a one-to-one correspondence between a single system administration database and an installed MQ Workflow server. If you want to enable workflow more than one system administration database, you must install additional corresponding MQ Workflow servers.

Managing workflow user access

Identify workflow users to the IBM WebSphere MQ Workflow server. Define the access control lists that you need for all elements of the workflow.

"Synchronizing users with MQ Workflow"

"Defining access control lists" on page 531

Synchronizing users with MQ Workflow:

When you create, modify, or delete a user ID or group in IBM Content Manager or IBM Information Integrator for Content, you must also do the same on the IBM WebSphere MQ Workflow server.

User IDs and groups are synchronized automatically if the MQ Workflow server is running and the workflow service is enabled when you manage users or groups in IBM Content Manager. If the MQ Workflow server is not running or workflow is not enabled when you manage users in IBM Information Integrator for Content, you must synchronize the users with MQ Workflow or you get an error.

"Adding or updating users on MQ Workflow"

"Deleting users from MQ Workflow" on page 530

Adding or updating users on MQ Workflow:

Run the synchronization utility to add and update users from the system administration database to the MQ Workflow server.

The synchronization utility adds or updates users or groups that are in the IBM Content Manager database but that are not on the MQ Workflow server. Complete the following steps to run the synchronization utility:

1. Ensure that the MQ Workflow server is running.
 - If you manually installed the MQ Workflow server, open **Services** and check the status for MQ Workflow X.X - FMC (where X.X is the version of workflow that you installed). Then start the service if it is not started.
 - If you silently installed the MQ Workflow server, navigate to the WfInstall directory and run the batch file, CMBWFStart.bat to start the server.
2. Ensure that the two INI files (cmbsvcs.ini and cmbsvclient.ini) in the IBMCMROOT directory correctly indicate the location of the workflow server. Make sure that cmbsvcs.ini specifies LOCAL if your server is local, or REMOTE if the server is remote. The cmbsvclient.ini file must contain the server location.
3. If you have a remote workflow server, you must start the RMI server batch or shell files (cmbsvregist81.bat, or cmbsvregist81.sh). These files are on the product CD in the WfInstall directory and you should have copied them to your workstation during installation.
4. Change to the directory where you installed IBM Content Manager. The default directory is the IBMCMROOT directory.
5. Enter EIPUser2WF.bat.
6. Type the required information for the IBM Content Manager database name, user ID, password, and schema. After you type the required information, the synchronization utility copies any users and groups from IBM Information Integrator for Content to the MQ Workflow server.

Tip: If a user ID or group does not exist on the MQ Workflow server, you get an error if you attempt to delete it from IBM Content Manager with workflow enabled and the MQ Workflow server running. For example, you create a user ID or group in IBM Content Manager with the workflow service disabled. Then you enable the workflow service and try to delete the user ID or group. You receive an error stating that the user ID does not exist in the MQ Workflow server.

To correct the error, you must run the synchronization utility to synchronize the user IDs and groups, and then delete the user ID or group. Alternatively, you can disable workflow service and delete the user ID or group.

Related reference

"Finding IBMCMROOT" on page 571

Deleting users from MQ Workflow:

Run the **fmcibie** command to delete users from the MQ Workflow server that you previously deleted from the system administration database.

If you manage users or groups in IBM Content Manager, user IDs and groups are synchronized automatically if the MQ Workflow server is running and the workflow service is enabled. If the MQ Workflow server is not running or workflow is not enabled when you delete users or groups from IBM Content Manager, you must complete this task to delete the users or groups from the MQ Workflow server:

1. Create a text file.
 - To delete individual user IDs, name the file DeletePersons.fdl and include the following lines:

```

CODEPAGE 1252
FM_RELEASE V3R3 2
DELETE PERSON 'User1'
DELETE PERSON 'User2'
DELETE PERSON 'User3'

```

where *User1*, *User2*, and *User3* are the users that you want to delete. You can list as many users as needed.

- To delete user groups, name the file `DeleteGroups.fdl` and add the following lines:

```

CODEPAGE 1252
FM_RELEASE V3R3 2
DELETE ROLE 'Group1'
DELETE ROLE 'Group2'
DELETE ROLE 'Group3'

```

where *Group1*, *Group2*, and *Group3* are the groups that you want to delete. You can list as many groups as needed.

2. Save the file.
3. Enter the following command at a command prompt.

```
fmcibie -u admin -ppassword -i filename -f -o
```

where *filename* is either `DeletePersons.fdl` or `DeleteGroups.fdl`.

When you delete a user ID from IBM Information Integrator for Content with workflow service enabled, you might get the following error:

```
Failed to delete a user [RC=12]
```

If the delete user operation fails, the system generates the `IBMCMROOT\temp.log` file that provides details about the failure.

A common reason for this failure is that you are attempting to delete a user that did not exist on MQ Workflow. You can resolve this problem by disabling workflow service and attempting the delete operation again.

Tip: If you try to delete the user ID that you used to log in to MQ Workflow, the delete operation fails.

Related reference

"Finding IBMCMROOT" on page 571

Defining access control lists:

Define the access control lists that you need for all elements of the workflow process.

When you have a complete picture of the elements of your workflow process, you can design the access control lists that you need. In an advanced workflow, you use access control lists (ACLs) to allow appropriate users to access the elements of the workflow at appropriate times. You apply an ACL to the following workflow elements: start node, work nodes, stop node, value nodes, and worklists.

The following steps provide one way to determine the ACLs that you need for your workflow.

1. Identify user groups who are involved with this workflow. For the XYZ Insurance Company's claims process, you need the following user groups:

- Agent
 - Adjuster
 - Underwriter
 - Accountant
 - Assistant
2. Identify advanced workflow elements (nodes, worklists, and the workflow process) that the users must access during the process.
 3. Create a matrix of the user groups and the elements.
 4. In each cell of the matrix, identify the privileges that are required during the process execution, such as CRUD (create, retrieve, update, and delete) capabilities.
 5. Represent the required privileges as privilege sets, either provided by the product, or defined by you.
 6. Define access control lists for each of the workflow elements.

Related concepts

“Privilege sets” on page 507

“Access control lists” on page 472

Related tasks

“Creating privilege sets” on page 507

“Creating privileges” on page 477

“Creating access control lists” on page 471

Related reference

“Predefined privileges” on page 477

Defining an action list

You must define an action list to identify the specific actions for the client users to perform during the steps in your process. The actions that you create become menu choices that client users can select while working with your process.

1. “Creating an action”
2. “Creating an action list” on page 535

Creating an action

Create actions that users can perform on work items in the process.

You can create an action by completing the following steps:

1. Click **Workflow** from the tree view in the System Administration Client window.
2. Right-click **Actions** and then **New**. The New Action window opens.
3. Type a name for your action in the **Name** field. The name can be up to 32 alphanumeric characters. You cannot change the name after you create the action.
4. Optional: In the **Description** field, type a description of the action. Descriptions are helpful when you create a specialized action, for example, an action that applies to a specific set of work items. You might also want to include a description for actions that you can use at any time. Descriptions help you to differentiate your purposes for creating one action one way over another way.

The description that you type here displays in the system administration client when you view details.

5. Type a 1- to 30-character alphanumeric name in the **Display name** field. This name displays to eClient users as a menu choice, so you should make the name short and meaningful.
6. Optional: In the **Shortcut** field, type the keys that give users quick access to the action in a custom client. This shortcut also displays in the custom client menu.

Restriction: Shortcut settings in this field do not apply to the eClient, only to custom clients.

7. Optional: Select an icon for your action in the **Icon** field. If you do not know where your icon graphic is located, click **Choose file**. Click **Preview** to see what the graphic looks like.
8. Optional: In the **Audit comment**, type a description for later use when auditors track workflow processes.
9. In the **Application name** field, type the full file name of the JavaServer Pages or the name of the servlet that runs on the eClient or custom Web client application. For example, you might type ProcessClaims.jsp for JavaServer Pages or ProcessClaims for a servlet.
10. Click **OK** to create your action and close the window. Click **Apply** to save the action and keep the window open to create another action.

Action: An *action* specifies how a user can manipulate the work items in a worklist. You can create your own actions, or use any of the following IBM Information Integrator for Content system-defined actions:

CMclient_Start on Workflow

Users select this action to start a work item on a workflow process.

CMclient_Remove from Workflow

Users select this action to remove a work item that is currently on a workflow process from that process.

CMclient_Change Workflow

Users select this action to remove a work item from one workflow process and start it on another process.

CMclient_View Workflow info

Users select this action to view information about a selected workflow process.

CMclient_View Workflow Variables

Users select this action to view the variables of the selected workflow process. You define these variables when you define the workflow (in the Workflow Properties window) or when you define a value node (in the Workflow Value Properties window).

CMclient_Accept

Users select this action to effectively check out or lock the work item in order to perform some activity. After completing the activity, the user selects **Continue**.

CMclient_Continue

Users select this action to move a work item along in the process, either after they have taken another action or instead of taking another action.

CMclient_Accept & Continue

Users select this action to effectively check out or lock the work item in order to perform some activity; after the activity is complete the work item is unlocked and moves along in the process.

CMclient_Suspend

Users select this action to suspend a work item in the workflow process that it is currently on.

CMclient_Resume

Users select this action so that a suspended work item can resume moving through the workflow process that it is currently on.

After you create an action, you must include it in an action list to use it.

Viewing or modifying an action:

Restrictions:

- You cannot change the name of an action.
- You can modify only the description and display name for a system-defined action.

To view or modify a predefined action:

1. Click **Workflow** from the tree view in the System Administration Client window.
2. Click **Actions** and then right-click a predefined action and select **Properties**. The Action Properties window opens.
3. Optional: In the **Description** field, type a description of the action. Descriptions are helpful when you create a specialized action, for example, an action that applies to a specific set of work items. You might also want to include a description for actions that you can use at any time. Descriptions help you to differentiate your purposes for creating one action one way over another way. The description that you type here displays in the system administration client when you view details.
4. Type a 1- to 30-character alphanumeric name in the **Display name** field. This name displays to eClient users as a menu choice, so you should make the name short and meaningful.
5. Optional: In the **Shortcut** field, type the keys that give users quick access to the action in a custom client. This shortcut also displays in the custom client menu.

Restriction: Shortcut settings in this field do not apply to the eClient, only to custom clients.

6. Optional: Select an icon for your action in the **Icon** field. If you do not know where your icon graphic is located, click **Choose file**. Click **Preview** to see what the graphic looks like.
7. Optional: In the **Audit comment**, type a description for later use when auditors track workflow processes.
8. In the **Application name** field, type the full file name of the JavaServer Pages or the name of the servlet that runs on the eClient or custom Web client application. For example, you might type ProcessClaims.jsp for JavaServer Pages or ProcessClaims for a servlet.
9. Click **OK** to modify your action and close the window. Click **Apply** to save the action and keep the window open.

Copying an action:

Copying an action can help simplify the creation of additional actions.

Restriction: You cannot copy a system-defined action.

To copy an action, complete the following steps:

1. Click **Workflow** from the tree view in the System Administration Client window.
2. Click **Actions** and then right-click a predefined action and select **Copy**. The Copy Action window opens.
3. Type a name for your action in the **Name** field. The name can be up to 32 alphanumeric characters. You cannot change the name after you create the action.
4. Optional: In the **Description** field, type a description of the action. Descriptions are helpful when you create a specialized action, for example, an action that applies to a specific set of work items. You might also want to include a description for actions that you can use at any time. Descriptions help you to differentiate your purposes for creating one action one way over another way.
The description that you type here displays in the system administration client when you view details.
5. Type a 1- to 30-character alphanumeric name in the **Display name** field. This name displays to eClient users as a menu choice, so you should make the name short and meaningful.
6. Optional: In the **Shortcut** field, type the keys that give users quick access to the action in a custom client. This shortcut also displays in the custom client menu.

Restriction: Shortcut settings in this field do not apply to the eClient, only to custom clients.

7. Optional: Select an icon for your action in the **Icon** field. If you do not know where your icon graphic is located, click **Choose file**. Click **Preview** to see what the graphic looks like.
8. Optional: In the **Audit comment**, type a description for later use when auditors track workflow processes.
9. In the **Application name** field, type the full file name of the JavaServer Pages or the name of the servlet that runs on the eClient or custom Web client application. For example, you might type ProcessClaims.jsp for JavaServer Pages or ProcessClaims for a servlet.
10. Click **OK** to create your action and close the window. Click **Apply** to save the action and keep the window open to create another action.

Creating an action list

Build an action list from system-defined actions and actions that you created. You apply the action list to work nodes in your process and the worklists that you create.

To create an action list, complete the following steps:

1. Click **Workflow** from the tree view in the System Administration Client window.
2. Right-click **Action lists** and click **New**. The New Action List window opens.
3. Enter a name for your action list in the **Name** field. The name can be up to 32 alphanumeric characters. You cannot change the name after you create the action list.
4. Optional: In the **Description** field, type a description of the action list. The description that you type here displays in the system administration client when you view details.

5. Populate the list of actions on the right. You can select multiple actions by holding the Ctrl key and clicking each action.
 - Add one or more selected actions from the left list to the right by clicking **Add**.
 - Add all actions from the left list to the right by clicking **Add all**.
 - Remove one or more selected actions from the right list to the left by clicking **Remove**.
 - Remove all actions from the right list to the left by clicking **Remove all**.
 - Use the search fields to search for actions to add or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
6. Optional: You can create additional actions by clicking **Create New Action**.
7. When you finish creating the action list, click **OK** or **Apply**.

Action list: An *action list* is a set of actions that a user can perform on work items. You assign an action list to each node in a process to specify the actions that the user can take at that step in the process. In the eClient, the user right-clicks a work item to display the list of available actions. The list that displays depends on the action list that you specified for the node where the work item is currently located.

Consider what actions you want users to take on the contents of a work item during the workflow process. For example, a claims adjuster can accept a claims form or reject it as incomplete.

Viewing or modifying an action list:

You must ensure that your system has the most current actions available to your users.

If policies change in your business, you need to update action lists that you created in the past. You might also need to check the current state of action lists to see what actions they include.

To view or modify a predefined action list:

1. Click **Workflow** from the tree view in the System Administration Client window.
2. Click **Action lists** and then right-click a predefined action list and click **Properties**. The Action List Properties window opens.
3. Optional: In the **Description** field, type a description of the action list. The description that you type here displays in the system administration client when you view details.
4. Edit the list of actions on the right. You can select multiple actions by holding the Ctrl key and clicking each action.
 - Add one or more selected actions from the left list to the right by clicking **Add**.
 - Add all actions from the left list to the right by clicking **Add all**.
 - Remove one or more selected actions from the right list to the left by clicking **Remove**.
 - Remove all actions from the right list to the left by clicking **Remove all**.

- Use the search fields to search for actions to add or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
5. Optional: You can create additional actions by clicking **Create New Action**.
 6. When you finish the modification of the action list, click **OK** or **Apply**.

Copying an action list:

Copy an action list when you want to create an action list that has similar actions, or, if you want to rename a current action list.

To copy an action list, complete the following steps:

1. Click **Workflow** from the tree view in the system administration client.
2. Right-click **Action lists** and then right-click a predefined action list and click **Copy**. The Copy Action List window opens.
3. Enter a name for your action list in the **Name** field. The name can be up to 32 alphanumeric characters. You cannot change the name after you create the action list.
4. Optional: In the **Description** field, type a description of the action list. The description that you type here displays in the system administration client when you view details.
5. Edit the list of actions on the right. You can select multiple actions by holding the Ctrl key and clicking each action.
 - Add one or more selected actions from the left list to the right by clicking **Add**.
 - Add all actions from the left list to the right by clicking **Add all**.
 - Remove one or more selected actions from the right list to the left by clicking **Remove**.
 - Remove all actions from the right list to the left by clicking **Remove all**.
 - Use the search fields to search for actions to add or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
6. Optional: You can create additional actions by clicking **Create New Action**.
7. When you finish creating the action list, click **OK** or **Apply**.

Modeling the workflow graphically

To launch the graphical workflow builder, you must define a new process or modify an existing one. With the graphical workflow builder, you draw the workflow process using nodes and connectors.

Accessible workflow builder: You can create a workflow using the graphical builder or the table builder. The graphical builder allows you to create a workflow using moveable icons on a drawing surface. For those who cannot use the graphical builder, you can create workflow processes using the table builder. The table builder offers all of the same functions as the visual builder, but accessible from the keyboard.

1. “Defining a new workflow process” on page 540
2. “Defining nodes in the workflow process” on page 545
3. “Defining a collection point” on page 552

4. Optional: “Defining an exit condition connector” on page 556
5. “Verifying the workflow diagram” on page 557
6. “Checking in a workflow process” on page 558

Workflow builder tools

The Workflow Definition window of the graphical builder is a split frame window that displays the workflow process diagram at the top and the summary table at the bottom. You can reposition the split bar by dragging it. You can also view the diagram without the summary table by clicking **View > Table**.

Table 83 identifies and describes the tools available in the workflow builder.

Table 83. Summary of workflow builder tools










Icon	Description	Example
	A start node begins the workflow process. In addition, work is performed at this node. The process diagram must have only one start node.	A start node might correspond to the activity of scanning a submitted claim form into the system.
	A work node represents a point in the workflow process where work is performed.	A work node might correspond to the activity of submitting an adjuster report or reviewing a large insurance claim.
	A user exit routine node calls an external business application to use with work items on a workflow process. Values from the workflow process can then be passed to the business application, and control values from the business application can be passed back to the workflow process.	You might have a user exit routine that runs a fraud check against policy holders who have submitted large claims.
	A collection node waits for one or more external event conditions to be met before continuing a workflow. The external event conditions are defined using the event node. Any connector that exits out of a collection node has a list of required events that must occur before the workflow continues.	You might use a collection point to wait for all of the required documents for a claim (police report and adjuster report, for example) before continuing with the claim process. You use the collection node to gather the awaited documents and indicate where in the process the waiting occurs.
	An event node is an external event that is not directly controlled by workflow. The workflow must wait at the collection node until the event occurs or time expires.	Create event nodes for each of the awaited events for a collection point. If you cannot continue with the process until you receive a police report and an adjuster report, you create two event nodes.

Table 83. Summary of workflow builder tools (continued)

Icon	Description	Example
	A value node locates workflow values, which you defined in the Workflow Properties, in the workflow.	A claim that starts on a workflow requires a claim amount and you want the agent to enter that value. In the Workflow Properties, you create a value called Claim Amount and specify to prompt the user for the number. You create a value node at the position in the workflow process where you want to prompt the agent, in this case, at the beginning of the workflow.
	A sub-workflow node is a predefined workflow incorporated in this workflow.	You might have a separate business process that includes the required steps for paying approved claims. This process is a separately defined process that you can include in the insurance claim process with a subprocess node and in other applicable processes as necessary.
	A stop node ends the process. In addition, work is performed at this node. Every workflow process diagram contains one stop node.	A stop node might correspond to the activity of moving a completed claim to a backup storage system.
	An exit condition connector contains conditions that must be met for work to proceed down a path on a workflow as opposed to other possible paths. The exit condition connector uses values defined in the workflow value node.	You might use an exit condition connector to send the insurance claim through different routes in your process depending on the value of the Claim Amount variable.

You can view the names of the tools by clicking **View > Toolbar icon text**.

Workflow summary table

The summary table includes the following columns:

Activity

The type of node is displayed in this column.

Name The name associated with the node is displayed in this column.

Description

The description of a node is displayed in this column.

Enter When a activity has an assigned type, that type is displayed in this column.

Miscellaneous

If a match criteria associated with the activity exists, then that match criteria is displayed in this column.

Performer

Who performs the activity.

Member

The name of a group or user ID.

Action List

The action list name for this activity.

Notify The user ID to notify if an activity exceeds time allowed.

After The time allowed for an activity in seconds, minutes, hours, days, weeks, or years.

Route The number indicates the workflow route from one node to the next in the workflow diagram.

From The node that precedes the node in this row is listed in this column.

To The node that follows the node in this row is listed in this column.

You can rearrange the columns in the summary table by selecting the column title and dragging it to its new position. The columns can be resized by dragging to reduce or enlarge the column width.

If you want to locate a particular node in the summary table, select it in the workflow process diagram. If you want to locate a particular node in your process diagram, you can do so by selecting the node in the summary table. If you double-click in any column of the summary table, the details associated with the node display.

Defining a new workflow process

Define workflow properties and launch the graphical workflow builder where you can model the workflow process.

To define a new workflow process:

1. Right-click **Workflow Definitions** from the tree view in the System Administration Client window and click **New > Visual Builder**. The Workflow Properties window opens in front of the graphical builder for modeling the workflow process.
2. Enter a name for the workflow in the **Name** field. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements.
3. Optional: In the **Description** field, type a description of the workflow process.
4. Select an action list from the **Default action list** field. Each node that you create for this workflow has this action list by default.
5. Select an access control list from the **Default access control list** field. Each node that you create for this workflow has this access control list by default.
6. Optional: Select **Enable notification of user after deadline** if you want to notify a user if a workflow activity is overdue.
If you select this option, you must select the user to notify and how long a user has to perform an activity before the notification. Enter the number and select a unit of time that the current user has to complete the activity.
Each node that you create for this workflow has these notification settings by default.
7. On the Assign Default Performer page, select a default user or group who must perform work node activities in this process. The user or users that you select

must have access to the work nodes and the necessary privileges to perform the actions. From the list of users that appear in the window, select the group or user that must perform the activity.

- a. Under **Performer**, specify whether the activity is performed by the user who started the workflow, a single user, or a user group. If you select **Starting user**, skip the remaining steps on this page of the notebook.
 - b. From the **Import from access control list** field, select the access control list that contains the user or users that you want to select. This access control list is the default ACL from which you want to identify the users and groups who complete the activities of the workflow.
 - c. Under **Users or Groups**, select the user or group who must perform the activity.
8. Optional: On the Create Workflow Values page, define the variables and values that you plan to use when you design the workflow process. To use the variables and values that you define here in your workflow process, you must define value nodes. The variables and values that you define here are for the entire workflow process; you define value nodes to correctly place those corresponding variables and values within the process. Consequently, the value node tool is enabled only after you provide values on the Create Workflow Values page. For example, if you want a user to provide a claim number when a workflow begins, you might enter the following values.

Field	Value
User prompts	Claim Number
Variable names	claimnumber
Variable values	XYZ11111

To display a prompt to the user or show the user the value that you supply, select the **Show value dialog to user** check box. Then you create a value node at the beginning of your process to prompt the user.

Restriction: You cannot use the right and left brackets ([]), double quotation marks ("), the tilde (~), or single quotation marks (') within any of the fields.

9. Click **OK** to save the workflow definition.

After you finish defining a new workflow, you can use the graphical builder to diagram the workflow process.

After you save a workflow definition, you cannot modify it unless you check it out.

Workflow process: A *workflow process* is a series of steps through which work is routed. A workflow process contains at least one start node, one activity, and one stop node. Workflow processes can have as many steps as you want.

A workflow process diagram is a graphical representation of the flow of work within an enterprise. The diagram is composed of nodes and connectors. The nodes define the locations where work is processed, and the connectors define the path that work takes through the workflow process.

You can create a variety of workflow processes.

- You can create serial processes that take work from start to finish through a straight line, without any deviations. These serial processes consist of nodes and connectors attached in a straight line.

- You can create parallel workflow processes that allow you to direct work through different routes that occur simultaneously. A parallel workflow process consists of a node that has more than one connector to send work on multiple routes.

Checking out a workflow process:

When you check out a workflow process, IBM Information Integrator for Content extracts the most recent version of the workflow process and prevents other users from making changes to it while you have it checked out. To modify a workflow process, you must first check it out.

To check out a workflow process, complete the following steps:

1. Expand **Workflows** in the tree view of the system administration client.
2. Click **Workflow Definitions**. Previously defined workflow processes display in the details pane.
3. Right-click one of the workflow processes in the details pane and click **Checkout**. If a workflow process is already checked out, then you cannot select **Checkout** and the workflow process icon changes to indicate that the workflow is checked out.

The workflow process is checked out.

Tip: If you save your changes to a process while it is checked out, you cannot undo them; you cannot retrieve a previous version of the process. If you are unsure of your changes, copy the process and test your modifications on the copy.

Viewing or modifying a workflow process:

You must check out a workflow process before you can modify it.

Tip: If you modify a workflow and save the changes, these changes are permanent and cannot be undone. If you are unsure about any changes that you make, copy the workflow process to a new name and make modifications to the copied version of it. Then, when you are satisfied with the results, check out and delete the old one and copy the new one to the old workflow name. Instances of the workflow are not affected while you make changes, but after you delete the workflow, no new instances can use the workflow.

You can view or modify the properties of a workflow process by completing the following steps:

1. From the System Administration Client window, click **Workflow Definition** from the tree view to display a list of workflow definitions in the details pane.
2. Right-click an existing definition and select **Properties**. The graphical builder launches the workflow process.
3. Click **Edit > Workflow Properties**.
4. Optional: In the **Description** field, type a description of the workflow process.
5. Select an action list from the **Default action list** field. Each node that you create for this workflow has this action list by default.
6. Select an access control list from the **Default access control list** field. Each node that you create for this workflow has this access control list by default.
7. Optional: Select **Enable notification of user after deadline** if you want to notify a user if a workflow activity is overdue.

If you select this option, you must select the user to notify and how long a user has to perform an activity before the notification. Enter the number and select a unit of time that the current user has to complete the activity.

Each node that you create for this workflow has these notification settings by default.

8. On the Assign Default Performer page, select a default user or group who must perform work node activities in this process. The user or users that you select must have access to the work nodes and the necessary privileges to perform the actions. From the list of users that appear in the window, select the group or user that must perform the activity.
 - a. Under **Performer**, specify whether the activity is performed by the user who started the workflow, a single user, or a user group. If you select **Starting user**, skip the remaining steps on this page.
 - b. From the **Import from access control list** field, select the access control list that contains the user or users that you want to select.
 - c. Under **Users or Groups**, select the user or group who must perform the activity of this work node.
9. Optional: On the Create Workflow Values page, edit the variables and values that you plan to use in the workflow process. To use any new variables and values that you define here in your workflow process, you must define value nodes. The variables and values that you define here are for the entire workflow process; you define value nodes to correctly place those corresponding variables and values within the process. Consequently, the value node tool is enabled only after you provide values on the Create Workflow Values page.

If you make changes to existing values on this page, those changes are not automatically reflected in any corresponding value nodes that already exist. To ensure that the changes are inherited by the existing value nodes, you must open each corresponding value node and save it again. For example, if you want a user to provide a claim number when a workflow begins, you might enter the following values.

Field	Value
User prompts	Claim Number
Variable names	claimnumber
Variable values	XYZ11111

To display a prompt to the user or show the user the value that you supply, select the **Show value dialog to user** check box. Then you create a value node at the beginning of your process to prompt the user.

Restriction: You cannot use the right and left brackets ([]), double quotation marks ("), the tilde (~), or single quotation marks (') within any of the fields.

10. Click **OK** to save the workflow definition.

After you finish modifying the workflow definition, you can use the graphical builder to change the workflow process.

After you save a workflow definition, you cannot modify it unless you check it out.

Copying a workflow process:

Copy a workflow process when you want to modify a current workflow process, or when you want to create another workflow process with similar properties.

Tip: If you modify a workflow and save the changes, these changes are permanent and cannot be undone. If you are unsure about any changes that you make, copy the workflow process to a new name and make modifications to the copied version of it. Then, when you are satisfied with the results, check out and delete the old one and copy the new one to the old workflow name. Instances of the workflow are not affected while you make changes, but after you delete the workflow, no new instances can use the workflow.

If you want to copy a previously defined workflow, complete the following steps:

1. From the System Administration Client window, click **Workflow Definition** from the tree view to display a list of workflow definitions in the details pane.
2. Right-click an existing definition and click **Copy**. The Enter unique workflow name window opens.
3. Enter a new name for the workflow in the **Name** field. Two workflow definitions cannot have the same name.

All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements. The graphical builder launches the copied workflow process.

4. To change any of the copied properties for workflow, click **Edit > Workflow Properties**.
 - a. Optional: In the **Description** field, type or edit the description of the workflow process.
 - b. Select an action list from the **Default action list** field. Each node that you create for this workflow has this action list by default.
 - c. Select an access control list from the **Default access control list** field. Each node that you create for this workflow has this access control list by default.
 - d. Optional: Select **Enable notification of user after deadline** if you want to notify a user if a workflow activity is overdue.

If you select this option, you must select the user to notify and how long a user has to perform an activity before the notification. Enter the number and select a unit of time that the current user has to complete the activity.

Each node that you create for this workflow has these notification settings by default.

- e. Optional: On the Assign Default Performer page, select a default user or group who must perform work node activities in this process. The user or users that you select must have access to the work nodes and the necessary privileges to perform the actions. From the list of users that appear in the window, select the group or user that must perform the activity.
 - 1) Under **Performer**, specify whether the activity is performed by the user who started the workflow, a single user, or a user group. If you select **Starting user**, skip the remaining steps on this page.
 - 2) From the **Import from access control list** field, select the access control list that contains the user or users that you want to select.
 - 3) Under **Users or Groups**, select the user or group who must perform the activity of this work node.
- f. Optional: On the Create Workflow Values page, define the variables and values that you plan to use when you design the workflow process. To use the variables and values that you define here in your workflow process, you

must define value nodes. The variables and values that you define here are for the entire workflow process; you define value nodes to correctly place those corresponding variables and values within the process. Consequently, the value node tool is enabled only after you provide values on the Create Workflow Values page. For example, if you want a user to provide a claim number when a workflow begins, you might enter the following values.

Field	Value
User prompts	Claim Number
Variable names	claimnumber
Variable values	XYZ11111

To display a prompt to the user or show the user the value that you supply, select the **Show value dialog to user** check box. Then you create a value node at the beginning of your process to prompt the user.

Restriction: You cannot use the right and left brackets ([]), double quotation marks ("), the tilde (~), or single quotation marks (') within any of the fields.

g. Click **OK** to save changes to the workflow definition.

After you finish defining the workflow properties, you can use the graphical builder to make any changes to the workflow process itself.

After you save a workflow definition, you cannot modify it unless you check it out.

Defining nodes in the workflow process

You can define various nodes to represent activities and steps in your workflow process. Most often, you define work nodes.

“Defining a work node” on page 546

“Defining a start node” on page 547

“Defining a stop node” on page 548

“Defining a user exit routine node” on page 549

“Defining a value node” on page 550

“Defining a sub-workflow node” on page 552

Node: *Node* is a generic term for any discrete point in a workflow process. If you are building your process with the graphical workflow builder, nodes are represented by icons in the drawing pane. Node can refer to any of the following possible elements:

- Work node
- Start node
- Stop node
- User exit routine node
- Value node
- Sub-workflow node
- Collection node
- Event node

You connect the nodes with connectors. You can connect a single node with another single node, which forces work to move serially from one node to another.

You can connect a single node with multiple nodes, which allows work to move through multiple routes at once, a situation that is referred to as parallel processing or parallel workflow.

Defining a work node:

Define a work node to represent an activity that occurs during the workflow.

To create a work node:

1. Select the work node tool:
 - In the toolbar, click the **Create work nodes** icon.
 - Click **Tools > Work** from the menu bar.
2. Click in the builder area where you want to add the work node. A work node icon displays in the builder.
3. Click the Deselect tool from the toolbar so that you can select and manipulate icons in the builder.
4. Double-click the work node icon or its equivalent in the summary table below the graphical builder. The Work Node Properties window opens.
5. On the Define Activity page, identify and describe the work node.
 - a. Enter a name for the node in the **Name** field. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements.
 - b. Optional: Describe the node in the **Description** field.
 - c. Select an action list from the **Action list** field or retain the default selection. Only those that you defined previously are available.

Important: If you do not define an **Action list** for a work node, all of the standard actions, such as suspend, resume, and start on process, are disabled in the eClient. However, all of the process routing actions, such as continue, are still be enabled, even if an action list is not associated.

- d. Optional: Select **Enable notification of user after deadline** if you want to notify the selected user that the activity of this node has not completed based on the deadline that you set.
6. On the Assign Activity to Performer page, select who must perform the work node activity. The user or users that you select must have access to this work node and the necessary privileges to perform the actions. From the list of users that appear in the window, select the group or user that must perform the activity.
 - a. Under **Performer**, specify whether the activity is performed by the user who started the workflow, a single user, or a user group. If you select **Starting user**, skip the remaining steps on this page of the notebook.
 - b. From the **Import from access control list** field, select the access control list (ACL) that contains the users or user groups that you want to select. The ACL limits your selections here, but does not control access for any work items at this node. The ACL that displays by default is the access control list that you specified on the Assign Default Performer page in the Workflow Properties.

You cannot select a user or user group that is not included in an access control list.
 - c. Under **Users or Groups**, select the user or group who must perform the activity of this work node.

7. Click **OK** to save the work node definition.

If you are selecting and deleting a large number of work nodes (for example, over 100 work nodes, depending on the machine configuration) in the system administration client, you might experience slow performance. You are advised to use the API (`delWorkNode` method) to delete a large number of work nodes.

Work node: A *work node* is a step within a workflow process where work is performed by specified users or groups.

Defining a start node:

Define a start node to represent an activity that occurs at the beginning of the workflow.

After you define a workflow, the builder opens with a pair of start and stop nodes. Both the start node and stop node are like any work node in that one or more users must perform some activity that you define while work is at that node.

Tip: You can define only one start node, so the start node tool and menu item are disabled when there is a start node on the drawing pane. If you delete the start node from the drawing pane, the tool is enabled.

To define the start node, complete the following steps:

1. If you do not already have a start node, add one to the builder area.
 - a. Select the start node tool:
 - In the toolbar, click the **Create a start node** icon.
 - Click **Tools > Begin** from the menu bar.
 - b. Click in the builder area where you want to add the start node. A start node icon displays in the builder.
 - c. Click the Deselect tool from the toolbar so that you can select and manipulate icons in the builder.
2. Double-click the start node icon or its equivalent in the summary table below the graphical builder. The Start Node Properties window opens.
3. On the Define Activity page, identify and describe the start node.
 - a. Enter a name for the node in the **Name** field. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements.
 - b. Optional: Describe the node in the **Description** field.
 - c. Select an action list from the **Action list** field or retain the default selection. Only those that you defined previously are available.

Important: If you do not define an **Action list** for a work node, all of the standard actions, such as suspend, resume, and start on process, are disabled in the eClient. However, all of the process routing actions, such as continue, are still be enabled, even if an action list is not associated.

- d. Optional: Select **Enable notification of user after deadline** if you want to notify the selected user that the activity of this node has not completed based on the deadline that you set.
4. On the Assign Activity to Performer page, select who must perform the start node activity. The user or users that you select must have access to this start

node and the necessary privileges to perform the actions. From the list of users that appear in the window, select the group or user that must perform the activity.

- a. Under **Performer**, specify whether the activity is performed by the user who started the workflow, a single user, or a user group. If you select **Starting user**, skip the remaining steps on this page of the notebook.
- b. From the **Import from access control list** field, select the access control list (ACL) that contains the users or user groups that you want to select. The ACL limits your selections here, but does not control access for any work items at this node. The ACL that displays by default is the access control list that you specified on the Assign Default Performer page in the Workflow Properties.

You cannot select a user or user group that is not included in an access control list.

- c. Under **Users or Groups**, select the user or group who must perform the activity of this start node.

5. Click **OK** to save the start node definition.

Defining a stop node:

Define a stop node to represent an activity that occurs at the end of the workflow.

After you define a workflow, the builder opens with a pair of start and stop nodes. Both the start node and stop node are like any work node in that one or more users must perform some activity that you define while work is at that node.

Tip: You can define only one stop node, so the stop node tool and menu item are disabled when there is a stop node on the drawing pane. If you delete the stop node from the drawing pane, the tool is enabled.

To define the stop node, complete the following steps:

1. If you do not already have a stop node, add one to the builder area.
 - a. Select the stop node tool:
 - In the toolbar, click the **Create stop node** icon.
 - Click **Tools > Stop** from the menu bar.
 - b. Click in the builder area where you want to add the stop node. A stop node icon displays in the builder.
 - c. Click the Deselect tool from the toolbar so that you can select and manipulate icons in the builder.
2. Double-click the stop node icon or its equivalent in the summary table below the graphical builder. The Stop Node Properties window opens.
3. On the Define Activity page, identify and describe the stop node.
 - a. Enter a name for the node in the **Name** field. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements.
 - b. Optional: Describe the node in the **Description** field.
 - c. Select an action list from the **Action list** field or retain the default selection. Only those that you defined previously are available.

Important: If you do not define an **Action list** for a work node, all of the standard actions, such as suspend, resume, and start on process, are

disabled in the eClient. However, all of the process routing actions, such as continue, are still be enabled, even if an action list is not associated.

- d. Optional: Select **Enable notification of user after deadline** if you want to notify the selected user that the activity of this node has not completed based on the deadline that you set.
4. On the Assign Activity to Performer page, select who must perform the stop node activity. The user or users that you select must have access to this stop node and the necessary privileges to perform the actions. From the list of users that appear in the window, select the group or user that must perform the activity.
 - a. Under **Performer**, specify whether the activity is performed by the user who started the workflow, a single user, or a user group. If you select **Starting user**, skip the remaining steps on this page of the notebook.
 - b. From the **Import from access control list** field, select the access control list (ACL) that contains the users or user groups that you want to select. The ACL limits your selections here, but does not control access for any work items at this node. The ACL that displays by default is the access control list that you specified on the Assign Default Performer page in the Workflow Properties.

You cannot select a user or user group that is not included in an access control list.
 - c. Under **Users or Groups**, select the user or group who must perform the activity of this stop node.
5. Click **OK** to save the stop node definition.

Defining a user exit routine node:

Optional: Define a user exit routine node to send control to an external business application during the workflow.

Before you can create a user exit routine node, you must:

- Ensure that the system administration client is installed on the same machine as the workflow server.
- Develop and store the user exit routine.
- Define the necessary access control list or lists.

To create or modify a user exit routine, complete the following steps:

1. Select the user exit routine tool:
 - In the toolbar, click the **Create user exit nodes** icon.
 - Click **Tools > User Exit** from the menu bar.
2. Click in the builder area where you want to add the user exit routine. A user exit routine icon displays in the builder.
3. Click the **Deselect** tool from the toolbar so that you can select and manipulate icons in the builder.
4. Double-click the user exit routine icon or its equivalent in the summary table below the graphical builder. The User Exit Routine Properties window opens.
5. On the Define Activity page, identify and describe the user exit routine.
 - a. Enter a name for the node in the **Name** field. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements.

- b. Optional: Describe the node in the **Description** field.
- c. Select an action list from the **Action list** field or retain the default selection. Only those that you defined previously are available.

Important: If you do not define an **Action list** for a work node, all of the standard actions, such as suspend, resume, and start on process, are disabled in the eClient. However, all of the process routing actions, such as continue, are still be enabled, even if an action list is not associated.

- d. Optional: Select **Enable notification of user after deadline** if you want to notify the selected user that the activity of this node has not completed based on the deadline that you set.
- 6. Depending on the operating system where the user exit routine will run, click **Windows User Exit**, **AIX User Exit**, or **SUN User Exit**.
- 7. Identify a specific, predefined user exit routine.
 - a. Type the name of a user exit routine in the **Exit routine name** field. If you want to use a user exit routine that you used in other workflow processes, select the name from the **Exit routine name** list and the remaining fields are completed automatically.
 - b. In the **Fully qualified application name** field, enter the full path name for the executable (EXE) file that can execute your user exit routine.

Requirement: You can use only executable (EXE) files for the exit routine; you cannot use batch files. However, you can use an EXE file that launches a batch file.

- c. Optional: Type any parameters for the executable file in the **Parameters** field.
- d. Specify the directory path, depending on whether your user exit routine uses a dynamic link library (DLL) or shared library.
 - For user exit routines that do not use a DLL or shared library, specify the directory path of the executable file in the **Working directory** field. The content of the **Working directory** field is the same as that of the **Fully qualified application name** field, without the EXE file extension.
 - For user exit routines that use a DLL or shared library, select the check box **PC DLL** or **Shared Library** (depending on the operating system) and type the directory path of the executable file in the **Entry point name** field.
- 8. Click **OK** to save your user exit routine.

The user exit routine is defined to the workflow server.

Defining a value node:

Define a value node if you want to direct work based on values or user decisions.

Before you can create a value node, you must create default values for the workflow on the Create Workflow Values page of the Workflow Properties.

In the Workflow Properties, you defined all of the variables and values that you want to use for the entire workflow process; you must define value nodes to correctly place those corresponding variables and values within the process. To define a value node, complete the following steps:

1. Select the value node tool:
 - In the toolbar, click the **Create workflow value nodes** icon.

- Click **Tools > Values** from the menu bar.
- 2. Click in the builder area where you want to add the value node. A value node icon displays in the builder.
- 3. Click the Deselect tool from the toolbar so that you can select and manipulate icons in the builder.
- 4. Double-click the value node icon or its equivalent in the summary table below the graphical builder. The Workflow Value Properties window opens.
- 5. On the Define Workflow Value page, identify and describe the value node.
 - a. Enter a name for the node in the **Name** field. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements.
 - b. Optional: Describe the node in the **Description** field.
 - c. Select an action list from the **Action list** field or retain the default selection. Only those that you defined previously are available.

Important: If you do not define an **Action list** for a work node, all of the standard actions, such as suspend, resume, and start on process, are disabled in the eClient. However, all of the process routing actions, such as continue, are still be enabled, even if an action list is not associated.

- d. Optional: Select **Enable notification of user after deadline** if you want to notify the selected user that the activity of this node has not completed based on the deadline that you set.
- 6. On the Assign Workflow Value to Performer page, select who must perform the value node activity. The user or users that you select must have access to this value node and the necessary privileges to perform the actions. From the list of users that appear in the window, select the group or user that must perform the activity.
 - a. Under **Performer**, specify whether the activity is performed by the user who started the workflow, a single user, or a user group. If you select **Starting user**, skip the remaining steps on this page of the notebook.
 - b. From the **Import from access control list** field, select the access control list (ACL) that contains the users or user groups that you want to select. The ACL limits your selections here, but does not control access for any work items at this node. The ACL that displays by default is the access control list that you specified on the Assign Default Performer page in the Workflow Properties.

You cannot select a user or user group that is not included in an access control list.
 - c. Under **Users or Groups**, select the user or group who must perform the activity of this value node.
- 7. Optional: On the Modify Workflow Values page, edit the variables and values that you want to use for this value node. The Modify Workflow Values page is populated with the variables and values that you defined on the Create Workflow Values page of the Workflow Properties.

Restriction: You cannot use the right and left brackets ([]), double quotation marks ("), the tilde (~), or single quotation marks (') within any of the fields.

- 8. Click **OK** to save the value node definition.

If, after you create this value node, you make changes to the values it uses in the Workflow Properties, those changes are not automatically reflected in this

corresponding value node. To ensure that the changes are inherited by this value node, you must open this value node and save it again.

Defining a sub-workflow node:

Define a sub-workflow node if you want to include an existing workflow in this workflow.

Before you can create a sub-workflow in a process, you must define and check in the workflow process that you want to be the sub-workflow.

A sub-workflow node is a predefined workflow incorporated into another workflow. Sub-workflows are usually shorter workflows that complete smaller, yet complex, tasks of their own.

To define a sub-workflow, complete the following steps:

1. Select the sub-workflow node tool:
 - In the toolbar, click the **Create a sub-workflow node** icon.
 - Click **Tools > Sub workflow** from the menu bar.
2. Click in the builder area where you want to add the sub-workflow node. A sub-workflow node icon displays in the builder.
3. Click the Deselect tool from the toolbar so that you can select and manipulate icons in the builder.
4. Double-click the sub-workflow node icon or its equivalent in the summary table below the graphical builder. The Sub-workflow Node Properties window opens.
5. On the Define Sub-workflow page, identify and describe the sub-workflow node.
 - a. Enter a name for the node in the **Name** field. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements.
 - b. Optional: Describe the node in the **Description** field.
 - c. Select an action list from the **Action list** field or retain the default selection. Only those that you defined previously are available.

Important: If you do not define an **Action list** for a work node, all of the standard actions, such as suspend, resume, and start on process, are disabled in the eClient. However, all of the process routing actions, such as continue, are still be enabled, even if an action list is not associated.

 - d. Optional: Select **Enable notification of user after deadline** if you want to notify the selected user that the activity of this node has not completed based on the deadline that you set.
6. On the Sub-workflow Options page, select the previously defined workflow process to be this sub-workflow. Only previously defined workflow processes that are checked in to the workflow server are available in the **Sub-workflow name** field.
7. Click **OK** to save the sub-workflow node definition.

Defining a collection point

Optional: Define a collection point if there are events that are not driven by the workflow but that must occur for the workflow to complete.

Before you can create a collection point, you must create the federated folder that will collect the work items at the collection node.

1. "Defining a collection node"
2. "Defining an event node" on page 554
3. "Defining a collection event list" on page 555

Collection point:

A *collection point* is a special node at which a federated folder waits for arrival of other objects, such as documents or folders, or for specified conditions to be met.

A collection point does not correspond to a business task. The collection point collects required objects and sends them to another node. The objects are sent either when the list of folder contents is complete or when the time allotted to wait for the documents or folders has expired.

Consequently, documents do not display in a user worklist until the required information is available.

Before you can create a collection point, you must create a federated folder that can contain the gathered documents and folders. You must define the following three workflow nodes for each collection point:

- A collection node
- An event node
- Two or more connectors, called collection event lists. One of these connectors must be defined as a timeout route.

Defining a collection node:

Define a collection node as the container for the awaited documents and folders.

Before you can create a collection node, you must create the federated folder that will collect the work items at the collection node.

To define a collection node, complete the following steps:

1. Select the collection node tool:
 - In the toolbar, click the **Create collection nodes** icon.
 - Click **Tools > Collection** from the menu bar.
2. Click in the builder area where you want to add the collection node. A collection node icon displays in the builder.
3. Click the Deselect tool from the toolbar so that you can select and manipulate icons in the builder.
4. Double-click the collection node icon or its equivalent in the summary table below the graphical builder. The Collection Node Properties window opens.
5. On the Define Activity page, identify and describe the collection node.
 - a. Enter a name for the node in the **Name** field. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements.
 - b. Optional: Describe the node in the **Description** field.

- c. Optional: Select **Enable notification of user after deadline** if you want to notify the selected user that the activity of this node has not completed based on the deadline that you set.
6. Click **OK** to save the collection node definition.

Next, define the event nodes for this collection point.

Restriction: You can define a total of 21 branches for each collection node: 20 event nodes and one timeout branch. After you reach the limit, the builder disables the event node tool. If you require more than 21 events, you must define another collection node.

Related concepts

“Federated folder” on page 89

“Native entity” on page 89

Related tasks

“Creating a federated entity manually” on page 83

“Creating a federated entity with the wizard” on page 79

Defining an event node:

Define up to 20 event nodes to correspond to awaited events for this collection point.

Restriction: You can define a total of 21 branches for each collection node: 20 event nodes and one timeout branch. After you reach the limit, the builder disables the event node tool. If you require more than 20 events, you must define another collection node.

To define an event node, complete the following steps:

1. Select the event node tool:
 - In the toolbar, click the **Create event nodes** icon.
 - Click **Tools > User event** from the menu bar.
2. Click in the builder area where you want to add the event node. An event node icon displays in the builder.
3. Click the Deselect tool from the toolbar so that you can select and manipulate icons in the builder.
4. Double-click the event node icon or its equivalent in the summary table below the graphical builder. The Event Node Properties window opens.
5. Enter a name for the node in the **Name** field. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements.
6. Optional: Describe what type of information the event node requires in the **Description** field. For example, if you need to have two witness reports, you can describe the event node as 2 witness reports.
7. Select a federated folder that will contain the awaited items. The contents of the folder are evaluated to determine whether they meet the criteria you specify for this event.
8. From the **Federated Entity** list, select a federated entity to evaluate. The list contains all of the federated entities that are defined in the federated database. When you select a federated entity, the associated native entities display, by content server, in the **Mapped native entity** table.

9. In the **Quantity needed** field, type the number of federated entities to wait for. For example, if the process should wait for two witness reports, type the number 2.
10. Click **OK** to save the event node and close the window.

After you define an event node, you can add it to a collection event list. The collection event list contains each event that must happen for the work at a collection node to take a specific route. You must have, by default, a timeout node, otherwise, work on a workflow process cannot complete.

Related concepts

“Federated entity” on page 88

Related tasks

“Creating a federated entity manually” on page 83

Event node: An *event node* is set of criteria that specifies the objects or conditions that are required by a collection node. For example, XYZ Insurance needs to wait for a police report, adjuster report, and an appraisal before processing a claim request—each of these required pieces of paperwork corresponds to an event node in their workflow process. The claim process cannot continue until each of these pieces of paperwork is available.

You can define up to 20 event nodes for each collection point. If the criteria defined in the event node are not met in a specified amount of time, the federated folder that is waiting at the collection node follows the timeout route. (You define the timeout route in the Collection Event List window.)

Defining a collection event list:

Define a collection event list to determine the route from a collection point based on the events that occurred.

To define a collection event list, complete the following steps:

1. Select the connector tool.
 - In the toolbar, click the **Create connectors** icon.
 - Click **Tools > Directional connector**.
2. Click an existing collection node in the builder that you want to be the source of the connection.
3. Click an existing node in the builder that you want to be the target of the connection. An arrow displays, pointing from the collection point node that you specified as the source toward the node that you specified as the target.
4. Double-click the dashed connector or its equivalent in the summary table below the graphical builder. The Collection event list window opens.
5. Enter a descriptive name of this branch connector in the **Branch criterion description** field. This name displays next to the connector in the drawing pane. All names can have one to 32 alphanumeric characters. A name cannot begin with a number or have any special characters. The **OK** push button is not enabled if you type a name that does not conform to the naming requirements. For example, Wait for police report.
6. Decide whether this route is event-driven or timeout. Each collection node requires one timeout route so that work does not stop for an indefinite time.

To create an event-driven route:	To create a timeout route:
<ol style="list-style-type: none"> 1. Click Wait for events. 2. Enter a precedence value for this collection event list from 0 through 20. The number must be the next number in sequence from the last collection event list that you created. This value controls the evaluation sequence for this collection event list compared with other collection event lists that exit from the collection node. The collection event list marked as 0 is evaluated first to see whether the criteria have been met. If not, the others are evaluated in order of precedence value. If none of the criteria is satisfied before the timeout duration expires, the federated folder takes the timeout route 3. Select the event nodes that you want to wait for from the Available events list and click Add. To remove nodes, select those nodes from the Assigned events list, and click DELETE. Restriction: The Assigned events list can support only 1024 characters. The number of events that you can add to the collection event list is restricted by the available space. For example, if you have several event names with two letters, like e1 or e2, you can assign more events to the collection event list than if you had longer event names. 	<p>Click Wait for period and specify a time period, after which the federated folder continues on the workflow process.</p>

7. Click **OK** to save the collection event list and close the window.

After you define a collection node, an event node, and a collection event list, verify the workflow diagram. The verification results inform you of any problems with your workflow process.

Collection event list: A *collection event list* is the criteria that a collection point uses to determine which route the federated folder must follow. The collection event list is either a specified amount of time or a list of events, which are event nodes.

You must create at least two collection event lists: one with a timeout period (timeout route) and the other with a list of events that must occur for a federated folder to proceed (event-driven route).

Defining an exit condition connector

Optional: Define an exit condition connector to direct work based on specified values or conditions.

You must determine where to direct the flow of work when a user reaches a critical point of your workflow. At this critical point, you must decide what conditions must be met and what action needs to occur next.

Exit condition connectors allow you to direct work according to whether conditions are met or not. For example, if John receives an insurance claim that he must approve or deny, you can add an exit condition connector that will take the insurance claim to the Accounting department if John approves the claim or to a business application that produces a rejection letter if John denies the claim.

Important Requirement: To verify a workflow, you must have at least two exit condition connectors to one node and one of them must be set to **Otherwise route**.

To define an exit condition connector, complete the following steps:

1. Select the exit condition connector tool.
 - In the toolbar, click the **Create exit condition connector** icon.
 - Click **Tools > Exit connector**.
2. Click an existing node in the builder that you want to be the source of the connection.
3. Click an existing collection point in the builder that you want to be the target of the connection. An arrow displays, pointing from the node that you specified as the source toward the collection point that you specified as the target.
4. Double-click the connector or its equivalent in the summary table below the graphical builder. The Exit Condition Branch window opens.
5. Define the branch condition.

To define a branch to follow if an expression is true:	To define a route to take if all evaluated branches are false:
<ol style="list-style-type: none">1. Clear Otherwise route.2. Select a workflow value variable from the Variable list. (The N in Priority(N) indicates that you need to enter a number value for this variable.)3. Select an operator.4. Enter a value to evaluate the variable for in the Value field.5. If you plan to create additional conditions, select a Boolean operator from the And/Or list. Do not select an operator if this condition is the last or only condition that you want to set for this branch.6. Click Add to add the new condition. The condition displays in the list box. You cannot edit the conditions in the list box. Select Clear to remove all conditions from the list.	Select Otherwise route if you have already defined a branch from the same node and that branch has an associated expression to evaluate.

6. Click **OK** to save the exit condition connector.

Verifying the workflow diagram

You cannot check in a workflow process until it has been successfully verified. New or updated workflow processes are verified automatically before they are checked in. However, you can verify your process at any time by completing the following steps:

1. Click **File > Verify**. The Verify window opens.

2. Review the **Verification results** list for errors or success. If you have errors, complete the following steps:
 - a. If you need additional information about an error message, click the message. The associated incorrect action item or connector is highlighted in the diagram. If you double-click the error message, the window that contains the problem opens.

Note that not all the messages listed in the **Verification results** list prevent the workflow process diagram from being verified successfully. Some messages are simply warnings.
 - b. Correct any errors.
 - c. Click **Reverify** to ensure that there are no more errors.
3. Click **Close** to close the window. If you click **Close** while the verification process is running, the process stops and window closes.

Checking in a workflow process

When you check in a workflow process to IBM Information Integrator for Content, it is saved in the system administration database and the workflow database.

Before you can check in a workflow process, you must verify it.

You can check in a workflow process from inside the graphical builder by clicking **File > Check in**. To check in a workflow process from the System Administration Client window, complete the following steps:

1. Expand **Workflows** in the tree view.
2. Click **Workflow Definitions**. Previously defined workflow processes display in the details pane.
3. Right-click one of the workflow processes in the details pane and click **Checkin**. If you did not previously check out the workflow process, then you cannot select **Checkin**.

The workflow process is checked in and the icon changes accordingly.

Releasing the lock on a checked-out workflow process

When you check out a process, the workflow builder locks the workflow process so that other users cannot change it. When you release the lock on a process, other users can check out the workflow process.

You might want to release a process if you decide not to update a process that you checked out. However, any changes that you save while the workflow process is checked out remain in your local copy even after you release the lock.

If you check out the process again after releasing the lock, you overlay your previous local copy, including any changes you might have made.

To release a workflow process, complete the following steps:

1. Expand **Workflows** in the tree view of the System Administration Client window.
2. Click **Workflow Definitions**. Previously defined workflow processes display in the details pane.
3. Right-click one of the workflow processes that is checked out and click **Release**.

The workflow process is no longer checked out and the icon changes accordingly. If the icon does not change immediately, then click **Refresh**.

Defining a worklist

You create worklists to allow users access to work items in workflow processes.

Before you can create a worklist, you must first create the access control list that you want to use for it and the work nodes that you want to associate with it.

To define, filter, and sort work items in a worklist, complete the following steps:

1. Expand **Workflows** in the tree view of the System Administration Client window.
2. Right-click **Work Lists** and click **New**. The New Work List window opens.
3. On the Definition page, identify and define the properties for the worklist.
 - a. Enter a name for your worklist in the **Name** field.
 - b. Optional: In the **Description** field, type a description of the worklist.
 - c. From the **Access Control Lists** field, select an access control list. Only those that you defined previously display.
 - d. Enter the maximum number of documents that a user can view at one time in the **Maximum results** field. If you want to return all work items in a worklist, then you must type -1.
4. Optional: On the Filter page, define criteria to limit the work items that display in the worklist. Use the operators to define how the worklist filters the values that you use.

Requirement: When you use the operator IN, you must use single quotation marks (') around each value, separated by a comma (,) and surrounded by parentheses, for example, ('node1', 'node2'). When you use the operator, LIKE, you can use the asterisk (*) as a wildcard character.

Specify a value for one or more of the following fields to create a filter:

Owner

Limits the displayed work items by work item owner. When you define an owner, you must insert the prefix CMB_. For example, if you want to define the owner ABC, you must enter 'CMB_ABC'.

You can click the ... push button to the right of the field to open the User List window where you can select a user ID from a list or search for user IDs.

Description

Limits the displayed work items by work node description.

Node Limits the displayed work items by work node name. For example, if you want work items that are at Node1 to display in the worklist, you type 'Node1' in the **Node** field. When users access their worklists, they see only those work items that are at Node1.

Priority

Sorts work items by their priority. Enter a numeric value.

Work item state

Displays the current condition of work items at a work node. The states that you can select are: Ready, Running, Finished, Terminated, Suspended, Disabled, Checked_out, In_error, Executed, Planning, Force_finished, Terminating, and Suspending.

Workflow state

Displays the current condition of the workflow process. The states that you can select are: Ready, Running, Finished, Terminated, Suspended, Terminating, and Suspending.

Last modified time

Sorts work items according to their last update.

Received time

Sorts work items according to when they arrive at a specific work node in a specific workflow. For example, if you have a node that you use in more than one workflow, the received time shows the time that a work item enters a work node in the selected workflow.

5. On the Sort page, populate and sort the worklist. Press Ctrl and click to select more than one work item at a time.
 - a. Populate the worklist.
 - Add one or more selected filter items from the **Available items** list to the **Sort items** list by clicking **Add**.
 - Remove one or more filter items from the right list to the left by clicking **Remove**.
 - Use the search fields to search for items to add or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
 - b. Use the **Ascending** or **Descending** radio buttons to order the items in the **Sort items** list.
 - c. Click **Move Up** or **Move Down** to move selected items in the **Sort items** list.
6. When you finish creating the worklist, click **OK** to save the changes and close the window. Click **Apply** to save the changes and keep the window open.

Worklist

A *worklist* is a filter of available work items that are assigned to specific users or user groups. From the eClient or a custom Web client, your users access the workflow process from the worklist. Users complete required activities (which you defined with the nodes in the workflow process) for work items and move work items through your workflow process. The activities that your users perform combined with the criteria and properties that you defined for your workflow process, move work items through the process.

When you define a worklist, you can filter work items at each step in a single workflow process. Alternatively, you can define a worklist for work from different workflow processes.

A worklist definition includes the rules that govern the presentation, status, and security of its work items. You specify these rules for each worklist at the same time as you create the worklist. You must create an access control list (ACL) to manage the access to the worklist; in that ACL, users must have the WFWorklist privilege.

Work item

A *work item* contains the document or object that a user requires to complete a workflow activity. The user is unaware of the work item because the user works on the document or object it references, not on the work item itself. A work item contains a set of information such as document status, creation date and so forth.

A work item can refer to any content (documents or objects) from a content server. Some examples of such content from the XYZ Insurance scenario include claims forms, photographs, appraisals, and expert reports.

Viewing or modifying a worklist

To view or modify a predefined worklist:

1. Expand **Workflows** in the tree view of the System Administration Client window.
2. Click **Work Lists**, right-click a predefined worklist, and select **Properties**. The Work List Properties window opens.
3. On the Definition page, identify and define the properties for the worklist.

Restriction: You cannot directly change the name of an existing worklist. To change a worklist name, you must copy it, rename it, and delete the existing worklist.

- a. In the **Description** field, type or edit the description of the worklist.
 - b. From the **Access Control Lists** field, select an access control list. Only those that you defined previously display.
 - c. Enter the maximum number of documents that a user can view at one time in the **Maximum results** field. If you want to return all work items in a worklist, then you must type -1.
4. Optional: On the Filter page, define criteria to limit the work items that display in the worklist. Use the operators to define how the worklist filters the values that you use.

Requirement: When you use the operator IN, you must use single quotation marks (') around each value, separated by a comma (,) and surrounded by parentheses, for example, ('node1', 'node2'). When you use the operator, LIKE, you can use the asterisk (*) as a wildcard character.

Specify a value for one or more of the following fields to create a filter:

Owner

Limits the displayed work items by work item owner. When you define an owner, you must insert the prefix CMB_. For example, if you want to define the owner ABC, you must enter 'CMB_ABC'.

You can click the ... push button to the right of the field to open the User List window where you can select a user ID from a list or search for user IDs.

Description

Limits the displayed work items by work node description.

Node Limits the displayed work items by work node name. For example, if you want work items that are at Node1 to display in the worklist, you type 'Node1' in the **Node** field. When users access their worklists, they see only those work items that are at Node1.

Priority

Sorts work items by their priority. Enter a numeric value.

Work item state

Displays the current condition of work items at a work node. The states that you can select are: Ready, Running, Finished, Terminated, Suspended, Disabled, Checked_out, In_error, Executed, Planning, Force_finished, Terminating, and Suspending.

Workflow state

Displays the current condition of the workflow process. The states that you can select are: Ready, Running, Finished, Terminated, Suspended, Terminating, and Suspending.

Last modified time

Sorts work items according to their last update.

Received time

Sorts work items according to when they arrive at a specific work node in a specific workflow. For example, if you have a node that you use in more than one workflow, the received time shows the time that a work item enters a work node in the selected workflow.

5. On the Sort page, populate and sort the worklist. Press Ctrl and click to select more than one work item at a time.
 - a. Populate the worklist.
 - Add one or more selected filter items from the **Available items** list to the **Sort items** list by clicking **Add**.
 - Remove one or more filter items from the right list to the left by clicking **Remove**.
 - Use the search fields to search for items to add or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
 - b. Use the **Ascending** or **Descending** radio buttons to order the items in the **Sort items** list.
 - c. Click **Move Up** or **Move Down** to move selected items in the **Sort items** list.
6. When you finish modifying the worklist, click **OK** to save the changes and close the window. Click **Apply** to save the changes and keep the window open.

Copying a worklist

Copying a worklist can help simplify the creation of additional worklists.

To copy a worklist, complete the following steps:

1. Expand **Workflows** in the tree view of the System Administration Client window.
2. Click **Work Lists**, right-click a predefined worklist, and select **Copy**. The Copy Worklist window opens.
3. On the Definition page, identify and define the properties for the worklist.
 - a. Enter a new name for your worklist in the **Name** field.
 - b. Optional: In the **Description** field, type a description of the worklist.
 - c. From the **Access Control Lists** field, select an access control list. Only those that you defined previously display.
 - d. Enter the maximum number of documents that a user can view at one time in the **Maximum results** field. If you want to return all work items in a worklist, then you must type -1.
4. Optional: On the Filter page, define criteria to limit the work items that display in the worklist. Use the operators to define how the worklist filters the values that you use.

Requirement: When you use the operator IN, you must use single quotation marks (') around each value, separated by a comma (,) and surrounded by

parentheses, for example, ('node1','node2'). When you use the operator, LIKE, you can use the asterisk (*) as a wildcard character.

Specify a value for one or more of the following fields to create a filter:

Owner

Limits the displayed work items by work item owner. When you define an owner, you must insert the prefix CMB_. For example, if you want to define the owner ABC, you must enter 'CMB_ABC'.

You can click the ... push button to the right of the field to open the User List window where you can select a user ID from a list or search for user IDs.

Description

Limits the displayed work items by work node description.

Node Limits the displayed work items by work node name. For example, if you want work items that are at Node1 to display in the worklist, you type 'Node1' in the **Node** field. When users access their worklists, they see only those work items that are at Node1.

Priority

Sorts work items by their priority. Enter a numeric value.

Work item state

Displays the current condition of work items at a work node. The states that you can select are: Ready, Running, Finished, Terminated, Suspended, Disabled, Checked_out, In_error, Executed, Planning, Force_finished, Terminating, and Suspending.

Workflow state

Displays the current condition of the workflow process. The states that you can select are: Ready, Running, Finished, Terminated, Suspended, Terminating, and Suspending.

Last modified time

Sorts work items according to their last update.

Received time

Sorts work items according to when they arrive at a specific work node in a specific workflow. For example, if you have a node that you use in more than one workflow, the received time shows the time that a work item enters a work node in the selected workflow.

5. On the Sort page, populate and sort the worklist. Press Ctrl and click to select more than one work item at a time.
 - a. Populate the worklist.
 - Add one or more selected filter items from the **Available items** list to the **Sort items** list by clicking **Add**.
 - Remove one or more filter items from the right list to the left by clicking **Remove**.
 - Use the search fields to search for items to add or remove from a list. Enter the first couple of letters of what you are looking for and click the search button. The search brings you the first instance of your query. Click the search button again to find the next instance of your query.
 - b. Use the **Ascending** or **Descending** radio buttons to order the items in the **Sort items** list.
 - c. Click **Move Up** or **Move Down** to move selected items in the **Sort items** list.

6. When you finish creating the worklist, click **OK** to save the changes and close the window. Click **Apply** to save the changes and keep the window open.

Troubleshooting system administration

System administration problems can occur in any of the components in the content management system, such as the clients, the DB2 database, the HTTP Server, the library server, and so on.

Understanding the IBM Content Manager and IBM Information Integrator for Content architecture can be beneficial in troubleshooting errors.

An IBM Content Manager system relies on many other software products and includes many components, for example:

- DB2 Universal Database
- DB2 Text Information Extender or DB2 Net Search Extender
- WebSphere Business Integration Server Foundation or WebSphere Application Server
- IBM HTTP Server
- IBM Content Manager library server
- IBM Content Manager resource manager
- Client for Windows
- IBM Content Manager eClient

Almost all of these products or components are interrelated, and either directly or indirectly communicate with each other. For example, when you use Client for Windows to perform a text search, the library server, the database, and text search are all used. If the text search fails, you must first determine where the failure occurred. You can usually make this determination by inspecting the error message.

For more help on troubleshooting your content management system, the IBM Support Web site provides several tools that you can download.

For example, the Log Analyzer is a plug-in for the IBM Support Assistant that helps you conveniently view logs for various IBM programs in one interface. After you install both the IBM Support Assistant and Log and Trace Analyzer plug-ins, you can import logs to the Log Analyzer tool and view them next to other logs. This view helps you compare log files from multiple applications. You can also filter the logs by severity, time stamp, process ID, and other attributes. For more information about IBM Support Assistant, the Log Analyzer, and other support tools, go to <http://www.ibm.com/software/support/isa/index.html?rcss=rtl>.

“Troubleshooting IBM Content Manager problems with the IBM Support Assistant” on page 566

“Troubleshooting the information center” on page 571

“Troubleshooting the system administration client” on page 577

“Troubleshooting the event monitor and event handler” on page 597

“Troubleshooting the library server” on page 600

“Troubleshooting the XML schema mapping tool” on page 625

“Troubleshooting the resource manager” on page 628

“Troubleshooting replication” on page 647

“Troubleshooting IBM Information Integrator for Content” on page 651

“Troubleshooting user authentication and access control” on page 659

“Troubleshooting LDAP integration” on page 666

“Troubleshooting document routing processes” on page 676

“Locale-specific considerations” on page 681

Related reference

“Tracing errors” on page 571

“Finding IBMCMROOT” on page 571

Troubleshooting IBM Content Manager problems with the IBM Support Assistant

For help with troubleshooting your content management system, the IBM Support Web site provides several tools that you can download.

The IBM Support Assistant is a workbench that provides you with tools that can help you with problem determination tasks. For more information about the IBM Support Assistant, the Log Analyzer, and other support tools, go to <http://www.ibm.com/software/support/isa/index.html?rcss=rtl>.

Downloading the IBM Support Assistant

To use the IBM Support Assistant tools, first download the IBM Support Assistant.

To download and install the IBM Support Assistant:

1. Go to the following Web site: <https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=isa>. Enter your IBM user ID and password. If you do not have a user ID, follow the instructions on the Web site to get a user ID.
2. Select the latest version of the IBM Support Assistant Workbench. Click **Continue**.
3. Select the appropriate version for your operating system, and click **Download now**.
4. Extract the ZIP or TAR file and run the setup program.

Installing the Content Manager EE plug-in

The Content Manager EE plug-in is a plug-in for the IBM Support Assistant that helps you gather trace information for Content Manager EE components and processes. These components and processes include the library server, resource manager, eClient, system administration client, Java API, JavaBeans, and installation and configuration processes. With this plug-in, you can enable and configure trace file options, gather the trace information, and choose whether to send the trace information to IBM Software Support.

The Content Manager EE plug-in is available in an English version only. It is available only for Content Manager EE and is not available for Content Manager for z/OS.

To install the Content Manager EE plug-in:

1. Start the IBM Support Assistant. On Windows, click **Start > All Programs > IBM Support Assistant > IBM Support Assistant Workbench**.

2. Open the Find New Products Add-ons window. This window opens automatically the first time that you start the IBM Support Assistant Workbench. Otherwise, click **Update > Find New > Product Add-ons**.
3. Expand **Information Management** and select **Content Manager Enterprise Edition**. Select the version that matches your current product version if multiple versions are listed. Click **Next**.
4. On the Tool Add-ons to Install page, click **Next**.
5. Accept the terms of the agreement. Click **Next**, then click **Finish**.
6. After the plug-in is installed, click **OK** and restart the IBM Support Assistant.

Collecting data with the Content Manager EE plug-in

To collect data about Content Manager EE components with the Content Manager EE plug-in:

1. Start the IBM Support Assistant and click **Launch Activity > Collect and Send Data**.
2. Select **Local Collection** to run the IBM Support Assistant on the local machine.
3. Expand the **Content Manager Enterprise Edition** plug-in for your version of Content Manager EE and select the component for which you want to gather data. Then click **Add** to add it to the Collector Queue.
4. In the Collector Queue, select the component and click **Collect All**.
5. Optional: If you want to configure the logs to re-create the problem, click **Yes** in the dialog box and configure the log information. After you provide information such as the logging level and log file size, click **OK** to return to the IBM Support Assistant and continue with the data collection.
6. View the results by clicking the **Current Status** tab.

Tip: To collect data from a remote machine, click **using IBM Support Assistant Lite** in the Remote Collection option. For more information about using IBM Support Assistant Lite on a remote machine, click the **More information** link on the interface.

Installing the Log Analyzer

The Log Analyzer is a plug-in for the IBM Support Assistant that helps you conveniently view logs for various IBM programs in one interface. After you install both the IBM Support Assistant and Log Analyzer plug-ins, you can import logs to the Log Analyzer tool and view them next to other logs. This view helps you compare log files from multiple applications. You can also filter the logs by severity, time stamp, process ID, and other attributes.

To install the Log Analyzer:

1. Start the IBM Support Assistant. On Windows, click **Start > All Programs > IBM Support Assistant > IBM Support Assistant Workbench**.
2. Open the Find New Products Add-ons window. This window opens automatically the first time that you start the IBM Support Assistant Workbench. Otherwise, click **Update > Find New > Product Add-ons**.
3. Expand **Information Management** and select the products that you are interested in. Select the correct edition and version if multiple editions and versions of a product are listed. Click **Next**. For example, select Content Manager EE, Content Manager for z/OS, or IBM Information Integrator for Content.

4. On the Tool Add-ons to Install page, select **JVM-based Tools > Log Analyzer**. Click **Next**.
5. Accept the terms of the agreement. Click **Next**, then click **Finish**.
6. After the plug-ins are installed, click **OK** and restart the IBM Support Assistant.

Analyzing log and trace files

To analyze your log and trace files with the Log Analyzer:

1. Start the IBM Support Assistant and click **Launch Activity > Analyze Problem**.
2. Click the **Tools** tab.
3. Select **Log Analyzer**. Click **Launch**.
4. Click **File > Import Log File**. Select Import from the local system.
5. From the **Log Types** menu, select **IBM Content Manager Server log**. Complete the remaining information in the Log Details tabs.
6. Click **OK**.

For long log files, you can use the Optimized Filter feature to limit the trace lines that are displayed. You can limit them by a selected time frame or by a specific severity level.

If the content management product that you want is not in the **Log Types** menu:

1. Shut down the IBM Support Assistant and the Log Analyzer.
2. To add the necessary Log Type components, extract the ZIP file ECMFamilyTrace to the following folder: C:\Program Files\IBM\IBM Support Assistant v3\plugins\com.ibm.ertools.ac.rcpla_4.4.0.20070810.
3. Restart the IBM Support Assistant and the Log Analyzer. The content management products should now be listed in the **Log Types** menu.
 “Information collected by the Content Manager EE Enterprise Edition plug-in data collection tool”
 “Log file locations” on page 570

Related reference

“Information collected by the Content Manager EE Enterprise Edition plug-in data collection tool”

Information collected by the Content Manager EE Enterprise Edition plug-in data collection tool

The data collection tool in the Content Manager EE Enterprise Edition IBM Support Assistant plug-in collects log data and other data for many product components and processes. These components and processes include the library server, resource manager, system administration client, eClient, Java API, JavaBeans, and installation and configuration processes.

Where file names are provided for the log files and other files in the following information, those names are the default names in Content Manager EE.

Data collected for the library server

The following data is collected for the library server:

- icmserver.log library server log file
- UDFTRACE text search log file
- results of the DB2 command db2diag

Data collected for the resource manager

The following data is collected for the resource manager:

- SystemOut.log file
- SystemErr.log file
- startServer.log file
- stopServer.log file
- icmmr.logfile resource manager log file (this file name might be appended with the process ID in a clustered environment)
- dsiterr.log Tivoli Storage Manager API log file
- api_trace.log file

Data collected for the system administration client

The following data is collected for the system administration client:

- cadmin.log file
- ldapimportutil.log file
- cmbxmle.log file
- cmbxmli.log file
- cmbemconfig.properties file
- cadmin.properties file

Data collected for the eClient

The following data is collected for the eClient:

- eClientTrace.log file
- IDM.properties file
- languageMapping.properties file
- IDMAadminDefaults.properties file
- javacore.*.txt file (such as javacore.date.time.txt on Windows)
- heapdump.*.phd file (such as heapdump.date.time.process_ID.phd on Windows)

Restriction: The javacore.*.txt file and heapdump.*.txt file are collected only if you are experiencing performance problems.

Data collected for the Java API and Java Beans

The following data is collected for the Java API and Java Beans:

- *user.name*.dklog.log file
- *user.name*.beans.log file

Data collected for the installation and configuration processes

The following data is collected for the installation and configuration processes:

- folder content of *IBMCMROOT/config/eclient*
- cmcfgecas.bat file in the *IBMCMROOT/config* path
- folder content of *IBMCMROOT/log*
- folder content of *IBMCMROOT/fixpack/cm/version/log*
- ECMInstallDataV8.xml installation data repository file

- results of the SQL command `select * from icmstlsupdatehist`
- results of the SQL command `select * from icmstsyscontrol`
- results of the SQL command `select * from rmversion`
- ICMSEVER.log library server log file
- db2diag.log file (DB2 only)
- results of the DB2 command `db2 get dbm cfg` (DB2 only)
- results of the DB2 command `db2 get db cfg` (DB2 only)
- results of the DB2 command `db2set -all` (DB2 only)
- listener.ora file (Oracle only)
- tnsnames.ora file (Oracle only)
- sqlnet.ora file (Oracle only)
- the value for the ORACLE_SID environment variable (Oracle only)
- results of the command `show parameters SERVICE_NAME` (Oracle only)
- spfileORACLE_SID.ora file and initORACLE_SID.ora file (Oracle only)

Log file locations

By default, the installation log files are in the *IBMCMROOT/log/PRODUCT* directory.

This section contains information about the logs for the various components of an installed and configured content management system.

Table 84. Log locations in IBMCMROOT/log

Product	Install log	Configuration log	Uninstall log
IBM Content Manager	cminstall.log	cmconfig.log	cmuninstall.log
IBM Information Integrator for Content	ii4cinstall.log	ii4cconfig.log	ii4cuninstall.log
eClient	ecinstall.log	ecconfig.log	ecuninstall.log
VideoCharger	vcinstall.log	n/a	vcuninstall.log

Client for windows log files

Log files from the Client for Windows are kept on the individual client for Windows systems. The location is a user preference, so it might vary from one system to another.

1. Connect the Client for Windows to the library server.
2. Select **Options > Preferences**.
3. Select **General**. The **Log File Directory** identifies the location of the client for Windows logs:
 - ICMClient.log
 - ICMClient.err
 - ICMClientLog.ini

System administration client logging

The system administration client logs error-level information to the *cmadmerr.log* file, which is located in the system administration client directory. You can change

the default parameters of the `cmadmin.log` file by using the common log control utility in the system administration client.

The IBM Information Integrator for Content component of the system administration client logs error information to the `dklog.log` file.

Tracing errors

You can turn on two types of logs, the event log and the trace log.

To turn on the event log, select the **Allow system administrator event logging** check box on the Log and Trace page of the Library Server Configuration window. Library server events are logged in the `ICMSTITEMEVENTS` table.

To turn on the trace log, select at least one of the check boxes on the page. The trace information is logged in the file displayed in the **Trace file name** field. You can select a different file name and set the maximum level allowed.

Tracing is done only when requested by client applications. It is also possible to directly update the system control table to trace all connections. For more information, contact IBM Software Support.

Finding IBMCMROOT

Many tasks to manage your content management system refer to the `IBMCMROOT` variable. You must know how to find the value of this variable.

Starting with Version 8.3, IBM Content Manager and IBM Information Integrator for Content both install to the same location, which is referred to as `IBMCMROOT`. `IBMCMROOT` is also used as an environment variable on the system.

- On UNIX, the location of `IBMCMROOT` is `/opt/IBM/db2cmv8`. This location is static and cannot be changed. There is also a working directory, `/home/user_name`, that contains some configuration and log files.
- On Windows, the default location of `IBMCMROOT` is `C:\Program Files\IBM\db2cmv8`. The working directory is optional. If no working directory is created during installation, the configuration and log files are written under `IBMCMROOT`.

`IBMCMROOT` replaces both `ICMROOT` (used for Content Manager Version 8.2 and earlier) and `CMBROOT` (used for Enterprise Information Portal Version 8.1 and earlier and Information Integrator for Content Version 8.2).

Troubleshooting the information center

Problems with the information center can include problems with the display of the information center and conflicts with other applications.

The information center contains HTML versions of the product documentation. It also provides the help for the system administration client.

This section describes how to solve common problems with the information center.

“Information center does not display” on page 572

“Information center topics display in English” on page 572

“Information center readme file not found” on page 573

“Information center welcome page not found” on page 573
“Information center page not found” on page 574
“Main eClient help topic not found in information center” on page 574
“Information center does not start on a system with only eClient installed” on page 575
“Commands to start and stop the information center not found” on page 575
“Java error when starting the information center” on page 576
“Information center conflict with other Windows applications” on page 576

Information center does not display

If the information center does not display, it might be configured to display in an incorrect browser.

Symptom

The information center and system administration client help do not display.

Possible cause

The information center is configured to display in the Netscape browser and the Netscape program was not found. The system administration client online help uses the information center.

Action

If you have Netscape installed, verify that it is in your path. If necessary, add it to your path.

If you do not have Netscape installed, you have two options:

- Install Netscape for use by the information center and system administration client online help.
- Create a symbolic link from your preferred browser to the typical Netscape installation location. For example:

```
ln -s /usr/bin/mozilla /usr/bin/netscape
```

Then add the Netscape location to your path.

Information center topics display in English

The display of English topics in a regional information center can be caused by different reasons.

Symptom

After launching the information center in your regional setting, some topics still display in English.

Possible cause

- A cached copy of the topic is displaying. This problem can happen even if your Web browser cache is disabled.
- If a translated version of a topic is not available, the topic displays in English rather than not at all.

Action

Refresh the topic in the browser. If it still appears in English, then it is not available in the selected language.

Information center readme file not found

If the information center readme file is not found, there might be a problem with the information center configuration.

Symptom

The **Information center** > **Readme** link does not resolve.

Possible cause

The information center configuration did not run during the installation. The configuration has a step that copies the `readme_nl.htm` file, where *nl* represents the language locale, over the `readme.htm` file.

Action

Perform one of the following actions:

- In the *IBMCROOT\infoctr* directory, delete the `readme.htm` file and rename the `readme_nl.htm` file to `readme.htm`.
- Reinstall the information center.

Information center welcome page not found

If the information center welcome page is not found, there might be a problem with the information center configuration.

Symptom

The welcome page in the information center does not display when the information center opens.

Attention: When the information center starts from a Help button in the system administration client, the page displayed is the online help for that window. Otherwise, a welcome page displays.

Possible cause

The information center configuration did not run during the installation. The configuration has a step that copies the `welcomecm.htm` file over the `welcome.htm` file.

Action

Perform one of the following actions:

- Delete the `welcome.htm` file and rename the `welcomecm.htm` file to `welcome.htm`.
For an information center in English, perform this step in the *IBMCROOT\infoctr\plugins\com.ibm.cmgmt.doc_8.4* directory.
For a translated information center, perform this step in the corresponding language subdirectory. For example, for the information center in German, the path is *IBMCROOT\infoctr\plugins\com.ibm.cmgmt.doc_8.4\de*.

- Install the information center again.

Information center page not found

If the information center is not found, then it might not be configured correctly or the service might be stopped.

Symptom

When launching a Web browser to the information center URL (for example, localhost:8081), the page cannot be found.

Possible cause

If the information center installation detects that 8081 is busy, then it increments the default to the next open port.

The information center configuration did not run during the installation.

The configuration has a step that starts the information center as a service (in Windows) or daemon (in UNIX). The information center configuration succeeded, but the service or daemon is stopped.

Action

Perform one of the following actions:

- Verify that the port number in the `IBMCMROOT\infoctr\cmcfgic.ini` file is the correct one to use.
- Start the information center from a command prompt with the **cmic_web_start** or **cmic_local_start** command. To stop the processes, enter **cmic_web_stop** or **cmic_local_stop**, respectively. These commands are in the `IBMCMROOT\bin` directory.
- Start the information center service. To start the UNIX daemon, enter `/bin/nohup etc/rc.cmcfgic -a start`. On Windows, start the Content Management Information Center service.

Main eClient help topic not found in information center

If the main eClient help topic is not found, there might be a problem with the information center configuration.

Symptom

The *Installing, Configuring, and Managing eClient* topic cannot be found.

Possible cause

The information center configuration did not run during the installation. The configuration has a step that renames the `plugin-false.xml` file to `plugin.xml` in the eClient directory.

Action

Perform one of the following actions:

- Find the *IBMCMROOT\infoctr\plugins\com.ibm.eclient.doc_version* directory, where *version* is the version of IBM Content Manager that is installed. Rename the *plugin-false.xml* file to *plugin.xml*.
- Reinstall the information center.

Information center does not start on a system with only eClient installed

If an information center with only eClient content does not start, there might be a problem with the information center configuration.

Symptom

In an eClient-only information center, the information center fails to launch because no documentation is found.

Possible cause

The information center configuration did not run during the installation. The configuration has a step that renames the *plugin-true.xml* file to *plugin.xml* in the eClient directory.

Action

Perform one of the following actions:

- Find the *IBMCMROOT\infoctr\plugins\com.ibm.eclient.doc_version* directory, where *version* is the version of IBM Content Manager that is installed. Rename the *plugin-true.xml* file to *plugin.xml*.
- Reinstall the information center.

Commands to start and stop the information center not found

If you cannot start and stop the information center, then there might be a problem with your path configuration.

Symptom

The following batch commands cannot be found: **cmic_web_start**, **cmic_local_start**, **cmic_web_stop**, and **cmic_local_stop**.

Possible cause

These commands are in the *IBMCMROOT\bin* directory, which must appear in your path.

Action

Perform one of the following actions:

- Append the directory to your path.

Windows

Add *%IBMCMROOT%\bin* to your path.

UNIX,

Add *\$IBMCMROOT/bin* to your path.

- Change to the *IBMCMROOT\bin* directory and execute the command from there.

Java error when starting the information center

If *IBMCMROOT* is not set, you might receive a Java error when you start the information center.

Symptom

The following error message is received after entering the **cmic_web_start** or **cmic_local_start** commands:

```
/infoctr/jre/bin/java not found
```

Possible cause

The command is trying to invoke Java from the *IBMCMROOT/infoctr/jre/bin/java* path, and *IBMCMROOT* is not set.

Action

Set *IBMCMROOT* to the location where you installed IBM Content Manager or IBM Information Integrator for Content.

Information center conflict with other Windows applications

The Content Management Information Center service might conflict with other Windows applications.

Symptoms

After installing the system administration client, certain applications no longer start.

Possible cause

There might be a conflict with the information center, which is started as a service on Windows.

Action

Try the following test:

1. If the information center is open, close the browser window.
2. Stop the Content Management Information Center service. Verify in the Services window that the service has stopped.
3. After the service is stopped, try to start the application that would not start.

If the application starts with the information center service not running, change the Content Management Information Center service from starting automatically to starting manually.

Important: If you disable automatic startup of the Content Management Information Center service, you must manually start it before you can use the information center. The information center provides the online help for the system administration client. If the Content Management Information Center service is not running, the **Help** buttons in the system administration client do not work.

Troubleshooting the system administration client

Problems with the system administration client might include problems with starting the client, logon problems, or problems with the setup and display of data.

“Unable to view newly modified information, even after clicking Refresh”

“Cannot retrieve objects when using characters outside the 7-bit ASCII range” on page 578

“System administration client help does not work” on page 579

“System administration client field-level help does not always display automatically” on page 579

“Troubleshooting administration client messages” on page 579

“System administration client does not start on UNIX” on page 582

“System administration client does not start on Windows” on page 582

“System administration client logon fails” on page 584

“System administration client logon fails after installing fix pack” on page 589

“System administrator cannot log on to z/OS” on page 589

“Invalid parameter error when creating or viewing an item type” on page 589

“OnDemand for AS/400 connection test fails” on page 590

“Content Manager server inventory viewer is empty” on page 590

“Displaying non-English display names for objects in the system administration client” on page 591

“Locating the IBM Content Manager database schema name using DB2 commands” on page 592

“Federated entities, search templates not displayed in administration client, APIs” on page 593

“Server connection test fails, system returns DGL0394A” on page 593

“Attribute sizing and string length considerations for non-English environments” on page 593

“Selecting and deleting work nodes can cause slow performance” on page 594

“Auto-linking race condition creates duplicate folders” on page 595

“XML import using the process interactively option” on page 595

“JAR file clash between WebSphere Application Server and XML services” on page 596

“IBM Content Manager components stop on Linux” on page 596

“Using IPv6 addresses in the system administration client” on page 597

Unable to view newly modified information, even after clicking Refresh

A problem with viewing newly modified information in the system administration client could be related to the way that API caching works.

Symptom

When you are logged on to the system administration client, you do not see newly modified information for administration objects from another session. Even after you click the **Refresh** tool button, you do not see this information. For example, some new attributes are created in another system administration client session or in another session by using the administration APIs. These new attributes are not displayed in your current session even when you click **Refresh**. The latest

information is only shown after you restart the system administration client.

Cause

Caching is turned on by default for the system administration client to improve performance. With this caching option turned on in the APIs level, the system administration client always gets objects from the APIs cache, instead of always getting them from the server when caching is turned off. Because caching is per connection session, information changed from another session is not updated in the cache of the current session.

The **Refresh** button only forces object retrieval from the APIs cache, instead of getting objects from its own cache in the system administration client. This behavior does not mean that the system administration client will retrieve objects from the server.

Action

If you have more than one system administration client or multiple administration API application sessions running at the same time, and some administration objects are changed, and you want to see the latest information reflected in each session, you must either restart each session or turn the cache option off before you start the system administration client. To turn off the cache for the system administration client, modify the `cmadmin.properties` file and add the following line to this properties file:

```
CacheOption=FALSE
```

You can find the `cmadmin.properties` file under your working directory:
WORKDIR/cmgmt/sa/ subdirectory.

Attention: With the cache option turned off, performance might be an issue depending on whether you have a long list of administration objects in your library server.

Cannot retrieve objects when using characters outside the 7-bit ASCII range

You cannot retrieve system administration objects or runtime objects when using characters outside the 7-bit ASCII range.

Symptom

Creating or updating objects by using characters outside the 7-bit ASCII range might result in objects on the server that cannot be retrieved or deleted. Affected objects can include system administration objects such as item types, users, or ACLs, or runtime objects such as documents or folders.

For example, your IBM Content Manager server is on *German_Windows* with code page 1252 and your Client for Windows is on *TCH_Windows* with Big5 code page = 950. If you create a user with the system administration client on the client machine by using Big5 characters, the creation appears to be successful. However, after the system administration client is refreshed, the user appears to have a blank name and any attempts to retrieve or delete the user fail.

Action

If you are using IBM Content Manager clients and servers on different code pages, you must use characters in the 7-bit ASCII range.

System administration client help does not work

If the system administration client help does not work, the information center service might not be running.

Symptom

The system administration client help does not work.

Possible cause

If the system administration client help does not display when you click **Help**, the service that starts the information center might not be running.

Action

The information center starts as a service on Windows. Make sure that the service has been started. See the information about starting Windows services for instructions.

Important: If you disable automatic startup of the Content Management Information Center service, you must manually start it before you can use the information center, which provides the online help for the system administration client. If the Content Management Information Center service is not running, the **Help** buttons in the system administration client will not work.

System administration client field-level help does not always display automatically

You can also use the F1 key or the Help button to display help topics.

Symptom

In the system administration client, the field-level help does not display automatically when the cursor is over some fields.

Action

If the field-level help does not display automatically, click the field or control and press F1 to display the field-level help. You can also click **Help** to display the help topic for the current window.

Troubleshooting administration client messages

Reviewing common system administration client messages and their causes and resolutions might help you solve system administration client problems more quickly.

The following error messages can help you identify and solve system administration client problems.

Table 85. System administration client error messages

Message	Possible cause	Action	Component
Adding an index from text server, {0}, would result in no available federated entity that contains mappings for all associated servers in the Selected Servers and Indexes table. You must create a federated entity that maps all the desired associated servers.	There is no federated entity available that contains mappings for all associated servers.	Create a federated object and map it to the associated text servers before creating a text index.	FedAdmin
A Java connector class was not specified in the server type definition. The connection cannot be made.	This error occurs when the user tries to connect to a DB server definition.	Check the server type definition to see if the specified class exists or is accessible.	FeNativeInventory.java FeServerBaseDialog.java
An error occurred while connecting to database {0} Make sure the database is running and configured correctly	The connection to the database you selected did not succeed.	Check with your system administrator for the status of the database and review configuration settings.	
An error occurred while reading the initialization file. Check your installation and environment setup.	The system was not able to read the application initialization (.INI) files.	Review the installation procedures and system configuration settings. Check file location and path names. If necessary, reinstall the application.	
An error occurred while retrieving {0} from the database.	The attempt to retrieve data from the selected database did not succeed.	Check with your system administrator for user permissions and database status.	
Criteria order is not set.	The Criteria order text field contains no value. It has to be filled with a valid value.	Specify a valid value in Criteria order text field.	FedAdmin
Criteria order must be greater than 0.	The value "0" is not valid for the criteria order. It must be greater than 0.	Replace the value in the Criteria order text field with a valid value.	FedAdmin
Display position is not set.	The Display position text field contains no value. It has to be filled with a valid value.	Specify a valid value in Display position text field.	FedAdmin
Display width is not set.	The Display width text field contains no value. It has to be filled with a valid value.	Specify a valid value in Display width text field.	FedAdmin
Display position must be greater than 0.	The value "0" is not valid for the display position, It must be greater than 0.	Replace the value in the Display position text field with a valid value.	FedAdmin
Display width must be greater than 0.	The value "0" is not valid for the display width. It must be greater than 0.	Replace the value in the Display width text field with a valid value.	FedAdmin

Table 85. System administration client error messages (continued)

Message	Possible cause	Action	Component
Error occurred, no message returned. Check Admin error log file.	An error message cannot be returned from the API or the server.	Review the details of the log file to determine the error.	
INTERNAL ERROR: requested template not found in the list.	Unexpected error occurred in system administration database. The requested template being deleted cannot be found in the database.	See your system administrator or IBM service representative.	FedAdmin
INTERNAL ERROR: criteria {0} is at unknown state, cannot be stored/updated.	Unexpected error occurred in the system administration database. The state of the specified criteria is corrupted.	See your system administrator or IBM service representative.	FedAdmin
Logon to server {0} failed. Enter a valid user ID and password.	The attempted logon to the content server did not succeed.	Repeat the logon procedure and enter a valid user ID and password.	
No server definition class is specified for {0} servers. Do you want to try the default server definition?	This error occurs when no dialog class is specified for the server type of a federated server.	Enter the server name or click Yes to accept the default.	FeServerCnObject.java
This attribute is already mapped. Cannot be modified or removed.	The attribute is already mapped to your content server's attribute, it cannot be modified or removed.	Remove the attribute mapping before modifying or removing the attribute.	FedAdmin
The connection to <i>content server</i> failed.	The attempted connection to your specified content server did not succeed.	<ul style="list-style-type: none"> • Check with your system administrator for network status. • Check network configuration settings. • Check that user permissions have been set. 	
The Java connector class, {0}, specified in the server type definition was not found.	The connection class cannot be found when trying to test the connection to a server or when creating a backend datastore.	Check the server type definition to see if the specified class exists or is accessible.	FeNativeInventory.java FeServerBaseDialog.java
The server definition class {0}, for {1} servers was not found.	A DB Class for the server cannot be found.	Check the server type definition to see if the specified class exists or is accessible.	FeJDBCServerDialog.java
The server inventory is empty.	The inventory data for this server is empty.	Run the Refresh server inventory action for the server.	FedAdmin

Table 85. System administration client error messages (continued)

Message	Possible cause	Action	Component
You must have a text server with inventory before creating a text index.	To create a text index, you must have a text server with inventory data defined on your system.	Create a text server on your system and run a server inventory for this text server.	

System administration client does not start on UNIX

Differences in the system CLASSPATH variable and your CLASSPATH variable might cause problems when you try to start the system administration client.

Symptom

The system administration client shell script relies on the system CLASSPATH variable to find the JDBC driver. The DB2 Universal Database installation sets the system CLASSPATH variable to include the JDBC driver. If you invoke the system administration client and overwrite the system CLASSPATH variable in your own CLASSPATH environment variable and your variable does not include the proper JDBC driver, then the system administration client will not be able to find the JDBC driver during logon.

Action

Be sure that your CLASSPATH variable does not overwrite the system CLASSPATH variable, or be sure that your CLASSPATH variable includes the proper JDBC driver.

System administration client does not start on Windows

There could be several different reasons if the system administration client does not start on Windows, including problems with directory access, the definition of the class path or system variables, or the length of the command.

Symptom

The system administration client fails to start on Windows.

Possible causes

Directory access

The user ID that starts the system administration client must have write access to the directory where the client is installed, *IBMCMROOT\admin* common.

IBMCMROOT not defined

The *IBMCMROOT* system variable must be defined and must match the installation location.

Incorrect class path

To use the system administration client, you must have *db2jcc.jar* in your class path.

Command length

On a system running Windows 2000 Server, the class path might be too long. Windows 2000 Server limits the length of a command line to 2 KB (2048 characters). When the command to start the system administration client executes, the class path and three fully qualified JAR files are appended to the command. If the system administration client is installed in the default location, then the following information is added:

```
c:\Program Files\IBM\db2cmv8\admin\common\uamanager.jar;  
c:\Program Files\IBM\db2cmv8\admin\common\cmadmin.jar;  
c:\Program Files\IBM\db2cmv8\admin\common\sacommon.jar;
```

If the combined length of the command, your class path, and the fully qualified JAR files exceeds the limit, the system administration client will not start.

Actions

Directory access

Verify that the user ID you logged in with has write access to the *IBMCMROOT*\admin\common directory.

IBMCMROOT not defined

The *IBMCMROOT* system variable must be defined and must match the installation location. If it is not defined, a Missing resource message displays when you start the system administration client.

To verify that this environment variable is set:

1. Click **Start > Control Panel > System**.
2. In the System Properties window, click the **Advanced** tab.
3. Click **Environment Variables**.
4. In the Environment Variables window, verify that *IBMCMROOT* is listed with the system variables and that the value is the installation location of Content Manager EE. If *IBMCMROOT* is not defined or is defined incorrectly, add it or update it, as necessary.
5. Close the System Properties window.

Incorrect class path

Verify that db2jcc.jar is in your class path and that the location is correct.

1. Open a command window.
2. Enter the following command:
set classpath
3. Find the db2jcc.jar file in the output and make sure that the file is in that location. If it is not, update the class path.

Command length

If you are using Windows 2000 Server, check your class path. Review the class path for outdated or duplicate entries. If you cannot shorten your class path, consider one of these options:

- Specify an abbreviated class path when starting the system administration client.
 1. Open a command window.
 2. Locate the db2jcc.jar file:
 - a. Enter the following command:
set classpath

- b. Find the db2jcc.jar file in the output and note its path.
3. Change to the *IBMCROOT*\admin\common directory. For example:
`cd c:\Program Files\IBM\db2cmv8\admin\common`
4. Use the following command to set the class path for the current program window to only db2jcc.jar:
`set classpath=c:\absolute_path\db2jcc.jar;`
 Use the absolute path to the db2jcc.jar file on your system. For example:
`set classpath=c:\Program Files\sql1lib\java\db2jcc.jar;`
5. At the same command prompt, start the system administration client:
`cmadmin.bat`
- Reinstall the system administration client in a different location with a shorter path.

System administration client logon fails

If the system administration client logon fails, there are several possible causes, including problems with database setup and incorrect logon data.

Symptom

The system returns an error message when you try to log on to an administration database.

Possible causes

- The database connection parameter file contains incorrect information about the database.
- An incorrect user ID or password was provided.
- The database is not cataloged.

Actions

This section provides three actions you can take to help solve administration client logon failures.

1. Verify the information in the database connection parameter file.
 - a. Make a backup copy of the database connection parameter file.

Product	Filename
IBM Content Manager	cmbicmsrvs.ini
IBM Information Integrator for Content	cmbds.ini

- b. Open the database connection parameter file in a text editor.
 - c. Verify that the values defined for the connection parameters are correct for the database you are trying to connect to. The first set of values usually applies to the system administration database that was defined during installation. You can also run the server configuration utility to populate the values in the file.
2. Verify the user ID and password.
 Contact the owner of the system administration database that you are trying to connect to. Verify that the user ID and password you are typing have the right level of authority to log on to and administer the database.
3. Verify that the database has been cataloged. At a DB2 command prompt, enter:

list database directory

If the database is not listed, catalog it. See the information about connecting the administration client to the databases for specific instructions.

“Locating the connection parameter file”

“cmbds.ini parameters”

“cmbicmsrvs.ini parameters” on page 586

Related tasks

“Connecting to a remote database” on page 67

Locating the connection parameter file

Problems with the connection parameter file can cause problems with logging on to the system administration client.

The location of the database connection parameter files varies. To find the files, complete the following procedure:

1. Change to the *IBMCMROOT*/cmgmt directory.
2. View the contents of the cmbcmenv.properties file. The path indicated in the **CMCFGDIR** parameter is where you can find the connection parameter files. The files are:

Product	Filename
IBM Content Manager	cmbicmsrvs.ini
IBM Information Integrator for Content	cmbds.ini

cmbds.ini parameters

The connection parameter files define connections between parts of the content management system, such as the IBM Information Integrator for Content system administration client and the administration database.

The following list defines each parameter in the cmbds.ini file, which defines the connection parameters between the IBM Information Integrator for Content system administration client and the administration database.

FEDSERVER

Type the database name. The default name is ICMNLSDB.

If you are connecting to multiple remote databases, you must catalog each remote database before you add an entry to cmbds.ini. If you are connecting to multiple local and remote databases that are all named ICMNLSDB, type an alias name in this field. An alias provides a unique name that identifies the remote database on your workstation. Alias names have an eight-character limit. For example, if the remote database name is ICMNLSDB, an alias might be REMOTE1.

FEDSERVERREPTYPE

Type the option that matches your database and connection preference in this field. The value for this parameter must be in all uppercase characters.

DB2 Users connect to DB2 by using the privileges associated with their own user IDs, if possible. If the user ID does not have the correct privileges, the connection is made with the shared connection ID.

DB2CON Users connect to DB2 by using the shared connection ID.

ORACLE Users connect to Oracle by using the privileges associated with

their own user IDs, if possible. If the user ID does not have the correct privileges, the connection is made with the shared connection ID.

ORACON Users connect to Oracle by using the shared connection ID.

FEDSCHEMA

Type the schema name that was assigned to the database during installation. If you do not know the schema name, see the information about connecting the administration client to databases. The default schema name is ICMADMIN.

FEDSSO

If single sign-on was enabled when the database was created, type TRUE. If single sign-on was not enabled, type FALSE. The default setting is FALSE.

FEDDBAUTH

Specify where the user ID authentication takes place. If user authentication occurs on the server where the database is installed, type SERVER. If authentication occurs on the client, type CLIENT.

FEDREMOTE

Specify whether the server is remote. Type TRUE for a remote server or FALSE for a local server.

FEDHOSTNAME

The host name of the server where the database that you want to connect to is installed. Depending on your company's network configuration, you can type either an IP address or a domain name.

FEDPORT

Type the port number assigned to the database during installation. The default port number is 50000.

FEDREMOTEDB

Type the name of the database that was assigned during installation. The default name is ICMNLSDB.

FEDNODENAME

Type the name of the node.

FEDOSTYPE

Type the name of the operating system on the server where the database is installed.

AIX For AIX

LINUX For Linux

SUN For Solaris

WIN For Windows

OS390 For z/OS

FEDJDBC DRIVER

Type the Java Database Connectivity (JDBC) driver name.

FEDJDBCURL

Type the JDBC URL.

cmbicmsrvs.ini parameters

The connection parameter files define connections between parts of the content management system, such as the IBM Content Manager system administration client and the library server.

The following list defines each parameter in the cmbicmsrvs.ini file, the file that defines the connection parameters between the IBM Content Manager system administration client and the library server.

Important: For all parameters in the cmbicmsrvs.ini file, you can also provide a value in the connect_string parameter of the DKDatastoreICM::connect method. A value in the connect_String parameter takes precedence over a value in the cmbicmsrvs.ini file.

ICMSERVER

Type the database name. The default name is ICMNLSDB.

If you are connecting to multiple remote databases, you must catalog each remote database before you add an entry to the cmbicmsrvs.ini file. If you are connecting to multiple local and remote databases that are all named ICMNLSDB, type an alias name in this field. An alias provides a unique name that identifies the remote database on your workstation. Alias names have an eight-character limit. For example, if the remote database name is ICMNLSDB, an alias might be REMOTE1.

ICMSERVERREPTYPE

Type the option that matches your database and connection preference in this field. The value for this parameter must be in all uppercase characters.

DB2 Users connect to DB2 by using the privileges associated with their own user IDs, if possible. If the user ID does not have the correct privileges, the connection is made with the shared connection ID.

DB2CON Users connect to DB2 by using the shared connection ID.

Important: DB2CON is not supported in the cmbicmsrvs.ini file that is used by the system administration client.

ORACLE Users connect to Oracle by using the privileges associated with their own user IDs, if possible. If the user ID does not have the correct privileges, the connection is made with the shared connection ID.

ORACON Users connect to Oracle by using the shared connection ID.

Important: ORACON is not supported in the cmbicmsrvs.ini file that is used by the system administration client.

ICMSchema

Type the schema name that was assigned to the database during installation. If you do not know the schema name, see the information about connecting the administration client to databases. The default schema name is ICMADMIN.

ICMSSO

If single sign-on was enabled when the database was created, type TRUE. If single sign-on was not enabled, type FALSE. The default setting is FALSE.

ICMDBAUTH

Specify where the user ID authentication takes place. If user authentication occurs on the server where the database is installed, type SERVER. If authentication occurs on the client, type CLIENT.

ICMREMOTE

Specify whether the server is remote. Type TRUE for a remote server or FALSE for a local server.

ICMHOSTNAME

Type the host name of the server where the database that you want to connect to is installed. Depending on your company's network configuration, you can type either an IP address or a domain name.

ICMPORT

Type the port number assigned to the database during installation. The default connection port number for databases installed on AIX, Linux, Solaris, or Windows is 50000. For z/OS, it is 446.

ICMREMOTEDB

Type the name of the database that was assigned during installation. The default name is ICMNLSDB.

ICMNODENAME

Type the name of the node.

ICMOSTYPE

Type the name of the operating system on the server where the database is installed.

AIX For AIX

LINUX For Linux

SUN For Solaris

WIN For Windows

OS390 For z/OS

ICMJDBC DRIVER

Type the Java Database Connectivity (JDBC) driver name.

ICMJDBCURL

Type the JDBC URL.

ICMJNDIREF

Type the Java Naming and Directory Interface (JNDI) indirect lookup resource reference string for the WebSphere Application Server connection pool. This string is used when a connection is requested with the JNDI indirect lookup.

ICMDBVER

For an Oracle database, type the database version used on the client side.

10 For Oracle Database 10g.

11 For Oracle Database 11g.

The C++ API requires this value to use the correct archive libraries and compiler. If no value is specified, the default value is 10. This parameter is not used by a DB2 database.

ICMGMTSYSATTRTS

Specify whether to use Greenwich mean time (GMT) for the following system attributes: SYSROOTATTRS.CREATETS, SYSROOTATTRS.LASTCHANGEDTS, and SYSROOTATTRS.CHKOUTTIMESTAMP. Type TRUE to use GMT. If no value is specified, the default value is FALSE.

System administration client logon fails after installing fix pack

Different fix pack versions of IBM Content Manager and IBM Information Integrator for Content on the same server can cause problems with logging on to the system administration client.

Symptom

If you have IBM Content Manager and IBM Information Integrator for Content installed on the same server, and you only install a fix pack for one or the other, the system administration client does not display any server names in the **Servers** list on the login window.

Possible cause

You might have different fix pack levels for IBM Content Manager and IBM Information Integrator for Content.

Action

1. Check the product version and fix pack levels for IBM Content Manager and IBM Information Integrator for Content. Open a command prompt and change to *IBMCMOOT*.
2. Enter `cmlevel`. The system returns the product version information. For example, 8.2.0.20 means Version 8.2, with fix pack 2.
3. Install fix packs as required to synchronize the version levels.

System administrator cannot log on to z/OS

If the system administrator cannot log on to a z/OS library server, the ICMACCL job might have changed.

Symptom

When logging on to a z/OS library server from the system administration client, an error message displays.

Possible cause

The job ICMACCL, which populates both the compiled ACL and the permissions tables, has been changed. It now contains a step called PERM that opens a cursor and then performs a selection using that cursor.

Action

To execute this job successfully, the DB2 database administrator must complete the following steps:

1. Bind DSNUTIL.
2. Run the DB2 job DSNTIJSJG.

Invalid parameter error when creating or viewing an item type

If you are using components of IBM Content Manager that are at different versions, invalid parameter errors might occur when you are creating or viewing an item type.

Symptom

DGL0303A: Invalid parameter displays when you attempt to create an item type or view an existing item type. The error displays when the New Item Type Definition or Item Type Properties window opens because the system administration client is attempting to initialize the **Start on process** field.

Possible cause

You are using a DB2 Content Manager Version 8.2 system administration client to work with a library server that contains document routing processes that were created or modified using DB2 Content Manager Version 8.3.

Action

You must upgrade your system administration client to Version 8.3 to work with a library server that includes document routing processes that were created or modified using Version 8.3.

If your Version 8.3 library server includes document routing processes that were created with Version 8.2, you can continue to use the Version 8.2 system administration client to view them. You cannot modify or view those processes without upgrading the system administration client.

OnDemand for AS/400 connection test fails

If you receive an error when you test the connection of an OnDemand for AS/400 server, a parameter might be missing.

Symptom

The system returns an error message when you define an OnDemand for AS/400 server and click **Test Connection**.

Possible cause

The value STAYCONNECT=1 is not set in the **Additional parameters** field.

Action

1. Click **Servers**.
2. Right-click **New** and click **OnDemand**.
3. Enter the server IP address or IP network host name in the **Server name** field.
4. Click **Initialization parameters**.
5. In the **Additional parameters** field, enter STAYCONNECT=1;;
6. Click **Apply**.
7. Click **Test Connection**. If the connection fails, see the cmbadmerr.log.

Content Manager server inventory viewer is empty

If the server inventory viewer is empty, the schema name might be missing or incorrect.

Symptom

After defining an IBM Content Manager server, the server inventory viewer is empty.

Possible cause

The schema name might have been omitted or entered incorrectly when the connection to the server was defined. Server schema names are defined during installation. The default schema name is ICMADMIN.

The server inventory viewer displays a summary of the attributes and entities of each IBM Content Manager server that you define. Each attribute and entity is associated with a schema name.

The server inventory viewer can display only attributes and item types associated with the schema that was specified when the server was defined. If the schema name was omitted or entered incorrectly when the connection to the server was defined, the server inventory returns no information and the viewer is empty for that server.

Action

1. Click **Servers**. Right-click the Content Manager server that is returning the empty inventory.
2. Click **Properties** and click **Initialization Parameters**.
3. Type `SCHEMA=name` in the **Connection string** field.
4. Click **Test Connection**.
5. If connection succeeds, click **OK**. If connection fails, check that you have cataloged the Content Manager database.
6. Right-click the Content Manager server icon.
7. Click **Refresh Server Inventory**.
8. Click **Tools > Server Inventory Viewer**.
9. In the left column of the viewer, locate the server name you connected to. Scroll to the database name, for example, ICMNLSDB. Verify that the viewer displays entity, attribute, and other information. If the inventory is empty, the person who installed the database might have used a schema name other than the default name. To locate the schema name for the database, see the information about locating remote database connection information.

Displaying non-English display names for objects in the system administration client

If you have problems with an incorrect display name in the system administration client, check the language setting on the Library Server Configuration window.

Symptom

In the system administration client, a user defines a new language and translates the display name for the data modeling objects, but the **Display name** field in the Properties window is still shown in English.

Cause

The **Display name** field displays the description in the language specified as the default language setting in the Library Server Configuration window. By default, this language setting is English. Unless this setting is changed to another language, the **Display name** field value is always displayed in English.

Action

The default language setting in the Library Server Configuration window determines what language the **Display name** field is displayed in for the data modeling objects. Therefore, you must define a new language and change the **Language** field on the Definition page of the Library Server Configuration window to this new language. Then you must translate the display name of the data modeling objects. All of the **Display name** fields then appear in this language.

Locating the IBM Content Manager database schema name using DB2 commands

If a database is returning an empty server inventory, you might need to find the database schema name to help you troubleshoot the problem.

Determine the IBM Content Manager schema name by identifying, connecting to, and listing the tables contained in the database that is returning the empty server inventory.

1. Open a DB2 command prompt.

2. Enter:

```
list db directory
```

A list of the local and remote databases displays. Local databases are labeled *indirect*

3. Scroll through the database list. When you find the name of the IBM Content Manager database that is returning the empty server inventory, make a note of the database alias.

4. Scroll to the bottom of the database list. Enter:

```
connect to aliasname user user_ID using password
```

The database server, SQL authorization ID, and local alias information for ICMNLSDB display. For example, enter:

```
connect to ICMNLSDB user ICMADMIN using password
```

5. Enter:

```
list tables for user
```

A list of database tables, and the schema name associated with each table, displays.

6. Make a note of the schema name.
7. Return to the administration client. Follow steps 1 through 7 in “Content Manager server inventory viewer is empty” on page 590. If the server inventory viewer displays no information, see the cmbadmerr.log log file and contact IBM Software Support.

Federated entities, search templates not displayed in administration client, APIs

The display of federated entities and search templates might be affected by certain language settings.

Symptom

Some federated entities and search templates are not displayed in the administration client or listed by the APIs.

Possible cause

When IBM Content Manager and IBM Information Integrator for Content share the same administration database and users change the default language setting from US English (ENU) to any other language in IBM Content Manager, objects such as federated entities and search templates that are defined using any default language settings other than ENU are not displayed in the system administration client or listed using the APIs.

This problem does not occur if IBM Content Manager and IBM Information Integrator for Content are not sharing the same administration database. For example, if only IBM Information Integrator for Content or IBM Content Manager is installed, or the administration database is only used by IBM Information Integrator for Content or IBM Content Manager, the problem does not occur.

Action

If you share a common database, want to add a new language in the IBM Content Manager system administration client, and plan to use IBM Information Integrator for Content in the same administration database, then do not change the default language settings in the IBM Content Manager system administration client.

Server connection test fails, system returns DGL0394A

The connection test for a server might fail if the connector specification is set to remote.

Symptom

After creating a content server in IBM Information Integrator for Content, the connection test fails and returns a DGL0394A error.

Possible cause

The connector specification is set to remote in the `cmbcs.ini` file.

Action

To solve this problem, edit the `cmbcs.ini` file located in `IBMCMROOT` and change the respective connector setting to `local`.

Attribute sizing and string length considerations for non-English environments

The language setting enabled for the database can affect how IBM Content Manager handles characters in attributes and strings.

Symptom

In operations involving documents in a non-English national language environment, one of the following SQL errors might occur:

- SQL0311N The length of string host variable number <var-number> is negative or greater than the maximum.
- SQL0433N Value <value> is too long.
- SQL0302N The value of a host variable in the EXECUTE or OPEN statement is too large for its corresponding use.

Possible cause

The storage size needed for storing a national language character can depend on the language setting. The storage size needed in DB2 Universal Database could take up to 3 bytes in a DB2 database for Unicode (UTF-8) and up to 2 bytes in an MBCS locale database. For example, for a national language such as Chinese or Japanese, each national language character would take up 3-byte storage spaces in a DB2 database enabled for Unicode. However, the same Chinese or Japanese national language character would only take 2-bytes in a DB2 database enabled with the default Chinese or Japanese locale. IBM Content Manager attribute size is measured in the number of bytes, not in the number of national characters. This same problem might occur when setting any string value for an IBM Content Manager object. For example, the problem could occur when entering a value in the **User Description** field for a user.

Action

When defining an IBM Content Manager attribute that holds national characters, consider the possibility that the same national characters might require different storage size, depending on the code page of the database.

When defining character type of CHAR, VARCHAR, LOBs attributes in IBM Content Manager, each character length specified is 1 byte in size.

When setting a string value for other IBM Content Manager objects, such as the User Description for a user object, the string entered must be shortened to meet the length requirement.

Important: Calculate the correct length of bytes to allow for the possible expansion in a native or Unicode database code page.

Selecting and deleting work nodes can cause slow performance

The use of the system administration client to delete many work nodes can affect system performance.

Symptom

Users who select and delete many work nodes in the system administration client might experience slow performance. For example, many work nodes might be more than 100 work nodes, depending on the machine configuration.

Action

Use the API (`delWorkNode` method) to delete many work nodes.

Auto-linking race condition creates duplicate folders

An auto-linking race condition can create duplicate folders.

Symptom

There is a possible race condition when two users create a document with the same attribute values for attributes that are auto-linked to a folder at the same time. If the folder to be linked to does not exist when the documents are imported, it is possible that the folder for the first user will be created and the second user will also create a folder because the folder from the first user has not yet been committed and it is not found by the second user.

This race condition results in two duplicate folders on the system. The document created by the first user is only linked to the folder that the first user created. The document created by the second user is only linked to the folder that the second user created. Future documents that are created with the same attribute values for linked attributes are linked to both folders.

Action

Duplicate folders can be prevented if the folder to be linked to already exists on the system. Another way to prevent duplicate folders is to create a unique component index on the link attributes on the folder item type. The index causes the creation of the duplicate folder by the second user to fail. This failure to create the folder causes the creation of the item to fail. However, if the second user re-creates the document, it is successfully linked to the folder created by the first user.

XML import using the process interactively option

Problems with the interactive processing of the import of an XML file might be resolved by a manual edit of the XML file.

Symptom

When you use the **Process interactively** option to import an XML file, you might experience problems when you use the **Do not import** option to work with **user group/group data** pairs and **storage group/storage group data** pairs.

Possible cause

When you choose **Process interactively** to import an XML file that contains a **usergroup/group data** pair or a resource manager **storage group/storage group data** pair, there are some restrictions on how you can use the **Do not import** option. In the Import Preprocessor Results window, you can right-click an object and then select the **Do not import** option to remove it from the objects to be imported. However, if you select the **Do not import** option on a user group or a resource manager storage group and then click **Continue**, the actual import process might fail even though the preprocessor does not raise any warning. Also, the XML import function does not compare the details in the user group data and storage group data section.

Action

Manually edit the XML file. Delete the user group with corresponding group data elements and delete the resource manager storage group element with the corresponding storage group data element.

Manually compare the difference between the user group data/storage group data value in the source XML file and the properties of the same object in the target system through the Property window. Correct any unwanted conflicts, then start importing the XML file.

JAR file clash between WebSphere Application Server and XML services

Class path settings might result in a JAR file clash between WebSphere Application Server and XML services.

Symptom

WebSphere Application Server Version 5.1 and XML services (using the Eclipse XSD package) use Eclipse plug-ins and have a common JAR called `ecore.jar`. The version of `ecore.jar` used by WebSphere Application Server is different from one used by XML services. When the `ecore.jar` file from WebSphere Application Server is in the class path, then XML services does not work. The opposite is also true: if the version for XML services is in the class path, then WebSphere Application Server does not work.

Action

While running XML services, if there are any WebSphere Application Server class paths set, clear these class paths before setting the classpath for XML services to avoid a clash. To set the XML services class paths using `cmbenv81` environment files, follow these steps:

1. Clear the current class path.
2. Run `cmbenv81` with the `xmlsdk` option.

IBM Content Manager components stop on Linux

A problem with IBM Content Manager applications stopping on Linux is related to known behavior of the Linux kernel.

Symptom

When connecting to a local DB2 database on Linux, some IBM Content Manager applications might stop. These applications include user applications, the resource manager application server `icrmr`, and resource manager daemons.

Possible cause

This situation is related to documented behavior between the Linux 2.4 kernel and multithreaded DB2 applications.

Action

Create a remote DB2 database alias to point to the local database. The local applications can use this alias to access the DB2 database.

Tip: To determine what kernel the system uses, enter `uname -a` at a command prompt.

Using IPv6 addresses in the system administration client

In a dual-mode environment, using an IPv6 address in the system administration client causes errors.

Symptom

In a dual-mode environment, using an IPv6 address in the system administration client causes errors.

Action

Do not enclose IPv6 addresses in square brackets ([and]) when using them in the system administration client.

Related information

Enabling IPv6 dual-stack support

Troubleshooting the event monitor and event handler

Problems with the event monitor and event handler include problems with starting these components.

The following topics provide troubleshooting information about the event monitor and event handler.

“An event monitor instance has already been started”

“Encountered a database error” on page 598

“Initial context cannot be created” on page 598

“LDAP authentication for JMS fails” on page 599

“The cmbemconfig.properties file is missing some configuration data” on page 599

“The cmbemconfig.properties file cannot be found or is not accessible” on page 600

An event monitor instance has already been started

Only one instance of the event monitor can run at one time.

Symptom

An attempt to start the event monitor or handler fails with the following message: An event monitor instance has already been started. Only one instance can run at a time. Reset the event monitor flag in the system administration client.

Possible cause

An event monitor instance is already started. Only one instance can run at a time.

Action

Ensure that only one event monitor instance is running. Reset the event monitor flag in the system administration client.

Related tasks

“Starting and stopping the event monitor” on page 698

Encountered a database error

If you receive a database error when you start the event monitor or event handler, check your logon information and your database access.

Symptom

An attempt to start the event monitor or handler fails with the following message: Encountered a database error. This might be due to an incorrect user ID or password entry, or to an incorrect database being specified.

Possible cause

One or both of the following problems could be the cause of this error:

- You are using an incorrect IBM Content Manager user ID or password or an incorrect FileNet Business Process Manager user ID or password
- You are specifying a database for which you do not have access permissions or specifying a database that is not active.

Action

Ensure that you are using the correct IBM Content Manager or FileNet Business Process Manager user ID and password for the specified database and that you have access permissions for the specified database.

Related tasks

“Starting and stopping the event monitor” on page 698

Initial context cannot be created

Problems with starting the event monitor or event handler might be because of incorrect parameter values in the configuration file or because LDAP information is incorrect.

Symptom

An attempt to start the event monitor or handler fails with the following message: Initial context cannot be created

Possible causes

The **INITIAL_CONTEXT_FACTORY** and **PROVIDER_URL** parameters in the `cmbemconfig.properties` file are not valid, or the LDAP user ID or LDAP password is not correct.

Action

Ensure that the **INITIAL_CONTEXT_FACTORY** and the **PROVIDER_URL** parameters in the `cmbemconfig.properties` file are valid. When prompted, provide a correct LDAP user ID and password.

Related tasks

“Modifying the event monitor and event handler settings” on page 696

LDAP authentication for JMS fails

When you start the event monitor or event handler, ensure that you enter the correct LDAP user ID and password if LDAP is used for authentication.

Symptom

When starting the event monitor or event handler, LDAP authentication fails with the following error message: LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 52e, vece

Possible cause

You did not provide a valid LDAP user ID (principal) or the password (credential) when prompted by the event monitor or event handler.

Action

When prompted, ensure that you enter a valid LDAP user ID (principal) or password (credential).

Related concepts

“Managing users with LDAP” on page 435

Related information

LDAP security authentication with the JMS

The cmbemconfig.properties file is missing some configuration data

Problems with starting the event monitor or event handler might be because the cmbemconfig.properties file is missing some configuration data.

Symptom

An attempt to start the event monitor or handler fails with the following message: The cmbemconfig.properties file is missing some configuration data. You must specify the following properties for the cmbemconfig.properties file: INITIAL_CONTEXT_FACTORY, PROVIDER_URL, QUEUE_CONNECTION_FACTORY and QUEUE_NAME

Possible cause

One or more event monitor and event handler settings are not specified in the cmbemconfig.properties file, or the settings are incorrect.

Action

Ensure that the **INITIAL_CONTEXT_FACTORY**, **PROVIDER_URL**, **QUEUE_CONNECTION_FACTORY** and **QUEUE_NAME** parameters are specified correctly in the cmbemconfig.properties file. For the new settings to take effect, restart the event monitor and handler.

Related tasks

“Modifying the event monitor and event handler settings” on page 696

Related information

Event monitor

Event handler

The cmbemconfig.properties file cannot be found or is not accessible

To start, the event monitor and event handler must be able to find the cmbemconfig.properties file.

Symptom

An attempt to start the event monitor or handler fails with the following message:
The cmbemconfig.properties file cannot be found or is inaccessible.

Possible cause

The cmbemconfig.properties file is missing. It might not have been installed correctly when the event monitor was installed, or it might have been moved.

Action

Ensure that the cmbemconfig.properties file is in the following directory.

Windows

cmgmt\em

UNIX cmgmt/em

If the file is missing, you can use a text editor to recreate the file using valid event monitor and handler settings. For the new settings to take effect, restart the event monitor and handler.

Related tasks

“Modifying the event monitor and event handler settings” on page 696

Troubleshooting the library server

Common problems with the library server might include problems with connections, data import and export, text index and text search, and other database issues.

This section describes how to solve common problems with the library server.

The library server contains attributes (metadata), text search indexes, document routing information, and access control information. When a client performs a search, the resource manager is not involved. The library server is a DB2 database accessed by stored procedures.

If you are troubleshooting a problem related to searching or access control, begin by checking the library server log file. The library server dynamically generates access modules for item types and static queries. If the access modules cannot be generated, or if there is an underlying problem with the database manager, library server errors can occur.

"Connection to an Oracle library server database fails"
 "Query performance can be slow with a query on the SEMANTICTYPE condition" on page 602
 "DGL3608A error when trying to import documents into IBM Content Manager" on page 604
 "Cannot export an item type to a WSDL file" on page 604
 "System failed to retrieve large objects" on page 605
 "ICMRM transaction management failure" on page 606
 "Code page error during item creation" on page 607
 "Too many cursors returned during item retrieval" on page 607
 "Error DGL5390A for minimum string length violation" on page 608
 "Error LS RC 7015 SQL RC=-911 linked to concurrency control in the IBM Content Manager database" on page 608
 "Failure to import XML using DKDDO.from XML()" on page 610
 "Failure to enable database for text with DB2 Net Search Extender" on page 610
 "Failure to define an item type that has text searchable attributes" on page 611
 "Failure to change a text index" on page 611
 "Determining the status of an index update that appears to have hung" on page 612
 "Unable to index plain text documents when using the CTXSYS.INSO_FILTER or CTXSYS.AUTO_FILTER preferences for a library server using Oracle" on page 612
 "Specifying code pages for phrased text search of Thai language content" on page 613
 "Unexpected text search results for Thai phrases" on page 613
 "SQL0302N error when creating or updating a document" on page 614
 "Table space is in check pending state after adding or editing a foreign key on z/OS only" on page 617
 "Error loading libraries in a 64-bit environment" on page 618
 "DGL0394A error when trying to log on to the library server with the system administration client" on page 619
 "Error LS RC 7017 SQL RC -670 row length exceeded limit" on page 619
 "Insufficient space when creating a large number of item types and item type subsets" on page 620
 "Changing the host name the resource manager uses to communicate with the library server" on page 620
 "SQL error code -181: Asynchronous recovery process cannot delete the entries in ICMSTItemsToDelete table" on page 621
 "Transaction log file for the database is full" on page 621
 "DGL0394A error when connecting to an IBM Content Manager server using the system administration client" on page 622
 "Troubleshooting batch load utility problems for Content Manager for z/OS" on page 623

Connection to an Oracle library server database fails

If you cannot connect to an Oracle library server database, the library server might not be configured correctly.

Symptom

Connection to an Oracle library server database fails with the following message:
Failure in loading native library db2jcct2, java.lang.UnsatisfiedLinkError:
db2jcct2 (Not found in java.library.path): ERRORCODE=-4472, SQLSTATE=null

Possible cause

The library server name was not found in the cmbicmsrvs.ini file.

Action

Add the Oracle library server to the cmbicmsrvs.ini file by running the Server Configuration Utility. If the library server is already defined in the cmbicmsrvs.ini file, you might need to modify the **ICMSERVER** parameter depending on which type of connection you are using:

IBM Information Integrator for Content C++ connectors

If you use the IBM Information Integrator for Content C++ connectors to connect to an IBM Content Manager library server on Oracle, then the value of the **ICMSERVER** parameter for the library server must match the *ORACLE_SID* name that corresponds to your library server database.

IBM Information Integrator for Content Java connectors

If you use the IBM Information Integrator for Content Java connectors to connect to an IBM Content Manager library server on Oracle and there is no value specified in the **ICMJDBCURL** parameter, then the value of the **ICMSERVER** parameter for the library server must match the *ORACLE_SID* that corresponds to your library server database.

Related concepts

JDBC connection string support in Oracle

Query performance can be slow with a query on the SEMANTICTYPE condition

If the number of documents on the system is large, queries on the SEMANTICTYPE condition might take a long time complete.

Symptom

The performance of a query of the library server database that includes the SEMANTICTYPE condition might be slow if there are many documents in the content management system. The number of documents in a system that could cause this problem to occur is based on several factors, including system resources on the hardware of your content management system. However, an estimate of this number is 1,000,000 documents.

For example, if you are also using IBM Document Manager with IBM Content Manager, then when you log on to the IBM Document Manager Desktop client, the logon process might be slow. There could be a long wait time while the IBM Document Manager Desktop client retrieves the folder list from the library server. This problem occurs because the IBM Document Manager Desktop client issues the following query to search for all folders and non-document items in the content management system:

```
/* [(@SEMANTICTYPE = 2 or @SEMANTICTYPE = 0)
and INBOUNDLINK[@LINKTYPE = "Contains"]/@SOURCEITEMREF = "A1001001A06G14B32249D43305"]
```

The query generates an inefficient SELECT statement that causes a table scan on the part system tables, and that action causes the performance problem.

Actions

To avoid this problem, you can create indexes on the SEMANTICTYPE and ITEMID columns in the ICMSTITEMS001001 and ICMSTITEMVER001001 tables. These new indexes can help improve the query performance.

To create the indexes for the ICMSTITEMS001001 and ICMSTITEMVER001001 library server database tables:

1. Run one of the following sets of commands to create the indexes, where *CREATOR* is the library server administrator ID. Run only the commands that apply to your database type:

Remember: If there are many items and parts in your content management system (that is, many rows in the ICMSTITEMS001001 table), the creation of the indexes might take a long time.

Table 86. Commands to create the indexes for ICMSTITEMS001001 and ICMSTITEMVER001001

Database type	Commands
Content Manager EE with DB2	<pre> CREATE INDEX %CREATOR%.ICMSXITEMS0010015X ON %CREATOR%.ICMSTITEMS001001 (SEMANTICTYPE ASC, ITEMTYPEID ASC, INPROGRESS ASC) CREATE INDEX %CREATOR %. ICMSTITEMVER00103X ON % CREATOR %.ICMSTITEMVER001001 (SEMANTICTYPE ASC, ITEMTYPEID ASC) </pre>
Content Manager EE with Oracle	<pre> CREATE INDEX %CREATOR %.ICMSXITEMS0010015X ON %CREATOR%.ICMSTITEMS001001 (SEMANTICTYPE ASC, ITEMTYPEID ASC, INPROGRESS ASC) TABLESPACE %ICM_LS_DBICLSNDX% CREATE INDEX %CREATOR%.ICMSXITEMVER00103X ON %CREATOR%.ICMSTITEMVER001001 (SEMANTICTYPE ASC, ITEMTYPEID ASC) </pre>

Table 86. Commands to create the indexes for ICMSTITEMS001001 and ICMSTITEMVER001001 (continued)

Database type	Commands
Content Manager for z/OSwith DB2	<pre> CREATE INDEX ?CREATOR?.ICMSXITEMS0010015X ON ?CREATOR?.ICMSTITEMS001001 (SEMANTICTYPE ASC, ITEMYPEID ASC, INPROGRESS ASC) USING STOGROUP ?STOGROUP? PRIQTY ?PRIINDX? SECQTY ?SECINDX? BUFFERPOOL ?BPV4? CREATE INDEX ?CREATOR?.ICMSXITEMSVER00103X ON ?CREATOR?.ICMSTITEMVER001001 (SEMANTICTYPE ASC, ITEMYPEID ASC) USING STOGROUP ?STOGROUP? PRIQTY ?PRIINDX? SECQTY ?SECINDX? BUFFERPOOL ?BPV4? </pre>

2. Use the RUNSTATS command to update the table statistics for ICMSTITEMS001001. For example, run the following command, where *icmdbname* is the name of the library server database:

```

RUNSTATS TABLESPACE icmdbname.IV111LSTS TABLE ALL INDEX ALL
SHRLEVEL REFERENCE;

```

DGL3608A error when trying to import documents into IBM Content Manager

The DGL3608A error could indicate that a user with invalid permissions created an item type. The item type might appear to exist, but the attribute and view database tables were not created.

Symptom

After successfully creating new item types, a user receives a DGL3608A error when trying to import documents to them.

Cause

Item type creation failed because of invalid permissions. The item types were created with a user ID that was not able to create the necessary attribute and view database tables.

Action

Log on to IBM Content Manager as icmadmin. This user ID has create table permissions for the IBM Content Manager database. Delete the item types created by the other user ID and create them again.

Cannot export an item type to a WSDL file

You receive errors when you export an item type to a WSDL file by using the system administration client.

Symptoms

When you try to export an item type to a WSDL file with the system administration client, the following error message displays: Can't find bundle for base name cmbxmlservices, locale en_US

Causes

The cmbwebservices.properties and cmbxmlservices.properties configuration files are not in the IBM Content Manager working directory.

Resolving the problem

Check whether cmbwebservices.properties and cmbxmlservices.properties exist in the IBM Content Manager working directory. The working directory is a common location in which to store files that are created or updated at run time.

If the cmbwebservices.properties and cmbxmlservices.properties files do not exist in the working directory, you must install and configure the Web services server component through the IBM Information Integrator for Content installer. You can select this component for configuration only if you have already configured other components.

Related reference

“Finding IBMCMROOT” on page 571

System failed to retrieve large objects

Prevent errors when saving large objects by setting your database options.

Symptom

The system runs out of storage when attempting to retrieve large objects. There is not enough storage space for the APP_CTL_HEAP_SZ parameter.

You receive one of the following messages when trying to retrieve a large object bigger than the current 25 MB defined size:

CTE0192 Errors occurred in an update index operation.

CTE0105 Memory allocation error.

CTE0101 A search engine operation failed.

Possible cause

The application control heap size configuration parameter (APP_CTL_HEAP_SZ) is not set high enough, or the user data limit is not set high enough.

Action for IBM Content Manager 8.4 and DB2 V8 fix pack 15 on AIX

Complete the following steps to tune your DB2 Universal Database environment.

1. Increase the size of the application control heap size configuration parameter (APP_CTL_HEAP_SZ).

You might have to set the value higher if you are running applications that use a lot of memory, if you have a system that contains a large number of database partitions, or if you use declared temporary tables. The amount of memory needed increases with the number of concurrently active declared temporary tables. A declared temporary table with many columns has a larger table

descriptor size than a table with few columns. So, having a large number of columns in the declared temporary tables of an application also increases the demand on the application control heap.

For more information about adjusting the application control heap size configuration parameter, see: <http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.admin.doc/doc/r0000102.htm>

2. Reset the user data limit.

To view the current user data setting, run the following command: `'/usr/bin/ulimit -a'`. You can run the command if you are the database instance owner. The soft user data limit on AIX is 128 MB.

Set the user data limit high enough to maximize the private memory available to DB2 Universal Database, but allow enough room for normal stack growth. For recommendations when setting the user data limit, see: Setting the user data limit for DB2 on AIX.

You must restart your instance for your change to be effective.

Action for a 32-bit system

1. Increase the size of the application control heap size configuration parameter (APP_CTL_HEAP_SZ).

You might have to set the value higher if you are running applications that use a lot of memory, if you have a system that contains a large number of database partitions, or if you use declared temporary tables. The amount of memory needed increases with the number of concurrently active declared temporary tables. A declared temporary table with many columns has a larger table descriptor size than a table with few columns. So, having a large number of columns in the declared temporary tables of an application also increases the demand on the application control heap.

For more information about adjusting the application control heap size configuration parameter, see: <http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.admin.doc/doc/r0000102.htm>

2. Reset the user data limit to unlimited.

Run the following command: `"ulimit -d unlimited <instance owner="">"`. Then run `"ulimit -a"`. For recommendations, see: Setting the user data limit for DB2 on AIX

You must restart your instance for your changes to be effective.

ICMRM transaction management failure

To continuously import items by using a single thread, you must have a WebSphere Application Server connection available.

Symptom

You receive the following message when continuously importing items using a single thread:

```
RMPersistenceConnectException: Connection not available,  
Timed out waiting for 180000.
```

Possible cause

WebSphere Application Server did not have any available connections.

Action

Tune your WebSphere Application Server data source by increasing the MAX connection number to 150.

1. Open the WebSphere Application Server administration console. For example: `http://hostname:9060/admin`.
2. Navigate to and change the following settings:
 - **Resources > JDBC > Data sources > icrmr_LS_database > Connection pools > 150**
 - **Resources > JDBC > Data sources > icrmr_database > Connection pools > Maximum Connections > 150**
3. Save and close.

Code page error during item creation

A code page error during item creation might result if the item has large string attribute values.

Symptom

You receive a code page error when you attempt to create items using the SDK C++ APIs. Typically, this problem occurs for items that have large string attribute values.

The error message is:

```
DKDatastoreAccessError (ID) 4294967295, Code: -334;  
SQL0334N Overflow occurred while performing conversion  
from codepage "819" to codepage "1208". The maximum size  
of the target area was "nnn" The source string length was  
"nnn" and its hexadecimal representation was "x'000..."  
[SQLExecDirect] [SQLCODE=-334,SQLSTATE=22524] (STATE):22524.
```

Possible causes

- The database was enabled for Unicode during installation.
- String attributes exist that have large values or are near the byte boundary for Unicode strings.

Action

Use binary (BLOB) attributes to contain Unicode data.

Too many cursors returned during item retrieval

The SQL RC=-954 error can be caused by an incorrect configuration of the APPLHEAPSZ parameter.

Symptom

During the retrieval of items, a user encounters library server error SQL RC=-954. This DB2 error indicates that the retrieve might have returned too many cursors.

Cause

The cause is incorrect configuration of APPLHEAPSZ. The APPLHEAPSZ parameter is set to 1024 from installation to allow for approximately 106 cursors to be opened.

Action

You can set the APPLHEAPSZ parameter to 15000 to allow a maximum of 1056 cursors to open concurrently.

From a DB2 command prompt:

1. To check the current value of APPLHEAPSZ, enter `db2 get db cfg for icmnlbdb | grep -i APPLHEAPSZ`.
2. To change the APPLHEAPSZ, enter `db2 update db cfg using APPLHEAPSZ 15000`.

Error DGL5390A for minimum string length violation

If you receive error DGL5390A, the minimum string length in the item type attribute and the original attribute might be different.

Symptom

An attribute that is defined in the item type or the component type has a minimum string length that is lower than or equal to your value. The VARCHAR attribute returns the error message DGL5390A:

Attribute named '*myAttribute*' contains a string of length '*actual string length*', which violates the minimum required length of '*some value*' specified in the attribute definition.

Possible cause

The system is enforcing minimum and maximum VARCHAR string lengths that are based on the original attributes that were defined before the item type that uses them.

Action

Modify minimum and maximum VARCHAR string length on the original attribute definitions. Short and integer attributes are not affected.

Tip: Adjustments appear in retrieved item type and component type definitions, but not in item type view or component type view definitions.

Related samples

For more information about attribute definitions, see the `SAttributeDefinitionCreationICM` API Education Sample.

For more information about item type definitions, see the `SItemTypeCreationICM` API Education Sample.

Error LS RC 7015 SQL RC=-911 linked to concurrency control in the IBM Content Manager database

In a concurrent environment, lock contention occurs because the database manager must ensure data integrity.

Symptom

When multiple users concurrently access the IBM Content Manager database for operations such as retrieval, insertion, update, and deletion, you might get the SQL error RC=-911 (SQL0911N) because of database lock contention.

In a concurrent environment, lock contention occurs because the database manager must ensure data integrity.

Possible causes

Lock contention might occur because of a timeout (reason code 68) or deadlock (reason code 2).

- *Timeout* means that DB2 was not able to lock a resource within the time specified by the LOCKTIMEOUT parameter. The IBM Content Manager default value for LOCKTIMEOUT is 30 seconds.
- *Deadlock* means that one application is waiting for another application to release the lock. The lingering application is locking the resource needed by the other.

Actions

Search the ICMSEVER.LOG log file for SQL0911N and -911 to identify the reason code. You can detect SQL0911N and avoid lock contention by performing one of the following tasks:

- Update the library server and resource manager database statistics and execution utilities REORG, RUNSTATS, REBIND to maintain good performance. You must bind the application again after successfully performing RUNSTATS.
- Ensure that your application has short transactions.
- When you define an item type, create an index for attributes that can be searched often. DB2 Universal Database uses indexes to retrieve the correct table row. When an index is absent, DB2 Universal Database must scan a table to meet the search criteria. Other applications can run concurrently, accessing the table being scanned, which could result in concurrency control issues.
- If two transactions attempt to operate on the same row, locking can occur. This problem can happen from a variety of functions. For example, if one user is creating a document (with a long-running transaction) and another user performs a search that checks that record, the second transaction will be locked out until the first transaction is completed. To determine whether this problem is the cause of an error, do these steps:
 1. Run the application with the library server trace level set to -15.
 2. Find the SQL error that reports the lock, and then find the item ID being accessed.
 3. Search further up in the log file to see if another user session is also operating on that item ID. In the server log, each session is identified by a unique string such as "?05161633031148".
- Ensure that all users have and use unique user IDs. If two users attempt to use the same user ID, locking can occur in functions such as checkout or document routing APIs.
- Set the following DB2 variable to avoid concurrency problems and improve performance of SQL update statements:

```
db2set DB2_EVALUNCOMMITTED=ON
db2set DB2_SKIPINSERTED=ON
db2set DB2_SKIPDELETED=ON
db2stop/db2start
```

Run the DB2 utilities REORG, RUNSTATS, and REBIND (after stopping and starting DB2) for this variable to take effect. This variable helps prevent deadlocks on DB2 Universal Database.

If the error persists, contact IBM Software Support for additional help with tuning your IBM Content Manager database.

Failure to import XML using DKDDO.from XML()

A failure to import XML by using DKDDO.from XML() might be because outdated persistent identifier information exists.

Symptom

You receive a failure when using DKDDO.fromXML() to import a document with parts from an XML file.

Possible cause

When you import a document with parts from XML by using the DKDDO.fromXML() interface, DKDDO.add() for the document returns an error if any parts exist. The parts might have outdated PID (persistent identifier) information that you must clear before you can create an item with the data that you import from the XML file.

Tip: You are not required to clear PIDs for the root and child components, but you can clear them as a precaution. You must not clear PIDs for reference attributes, folder contents, and linked items because they must reference items that already exist.

Action

Clear the document part PIDs and define the PIDs to appear as if they had just been created using the DKDatastoreICM.createDDO(0) method.

Related sample

For more information, see the TExportPackageICM API Education Sample.

Failure to enable database for text with DB2 Net Search Extender

A problem with enabling DB2 Net Search Extender might be related to an incorrect entry of the ID.

Symptom

When you attempt to enable the database for text, you receive error CTE0143:

The command requires database administration authority for user icmadmin. Failure occurs when attempting to enable a database for text.

Possible cause

You might have used mixed case or lowercase characters when entering the user ID required to enable the DB2 Net Search Extender. The application expects the user ID to be uppercase.

Action

Repeat the command and enter the user ID with uppercase characters.

Failure to define an item type that has text searchable attributes

A problem with the creation of a text searchable item type might be related to the status of DB2 Net Search Extender.

Symptom

You receive an error message when defining an item type that is classified as text searchable or that has user-defined attributes that are text searchable.

Possible cause

DB2 Net Search Extender is not started, or the database is not enabled for text searching.

Action

Start DB2 Net Search Extender on the library server workstation by performing one of the following steps:

- Open a DB2 command prompt and enter `db2text start`
- Enable the database for text searching. Open a DB2 command prompt and enter the information as shown in the following example:

```
db2text enable database for text connect to ICMNLSDB user userID  
using password
```

ICMNLSDB

Name of the database

userID Valid user ID

password

Password for the user ID

Failure to change a text index

A problem when updating a text index might be related to an expired password in DB2 Net Search Extender.

Symptom

You receive the following error while updating, reorganizing, or using text indexes for text searchable components:

DKUsageError:

DGL5203A: The password is invalid for the user ID used to administer text indexes. ICM7172: The password provided is invalid for this user ID, or it is NULL. (STATE): [LS RC=7172, SQL RC=-1].

Possible cause

Invalid or nonexistent DB2 Net Search Extender password.

Action

Set the DB2 Text Information Extender or DB2 Net Search Extender password using the system administration client.

1. Log on to the system administration client.
2. Expand the **Library Server Parameters** category in the left pane.
3. Select **Configurations** in the left pane. The library server configuration properties display in the right pane.
4. Click the **Features** tab.
5. Type the correct DB2 Text Information Extender or DB2 Net Search Extender user ID and password.
6. Attempt to update, reorganize, or use text indexes for text searchable components again.

Determining the status of an index update that appears to have hung

An index update that appears to take a long time might be the initial update of the index.

Symptom

With a library server that is using DB2, the following symptoms occur:

- After creating a text searchable item type and updating the index, the update command does not return if data is continuously modified.
- The NUMBER_DOCS column in DB2EXT.TEXTINDEXES does not show any additional documents added.

Possible Cause

The data is being loaded during the initial update of the index, which prevents any COMMITCOUNT value from being used. Before any data is loaded, the index must be manually updated to enable use of COMMITCOUNT for the index.

Action

There is no workaround. You can monitor the update process of a DB2 Net Search Extender index.

Unable to index plain text documents when using the CTXSYS.INSO_FILTER or CTXSYS.AUTO_FILTER preferences for a library server using Oracle

The resolution for a problem with documents that use the INSO_FILTER or AUTO_FILTER depends upon the type of content.

Symptom

When text documents are sent to the INSO_FILTER or AUTO_FILTER, they are assumed to be in the character set encoding specified by the locale of the server machine or the locale of the user that is used to run the Oracle processes. Problems occur when this assumption is not correct, because incorrect text is returned from the filter to OracleText, which results in the document not being searchable.

Action

Text-only content

If the resource content of either a resource item type or document item type will always be plain text, then it is better to set the filter to be `NULL_FILTER` (for the document in the same encoding as the database) or to use `CTXSYS.CHARSET_FILTER` to specify the character set of the documents.

Mixed content

It is possible to use a format column and specify `TEXT`, which causes `OracleText` to not send specific items to the filter.

Important: Specifying `TEXT` in the format column is supported only with resource item types. This setting requires that the format is set on the `DKTextICM` object before it is stored into IBM Content Manager.

You can use the system administration client to set the key/value pair for the format column. In the **Index Information** fields for the index, use the following values:

Option name

format column

Option value

format

You can also programmatically set this key/value pair using the `dkTextIndexICM` and `dkOracleTextIndexICM` interfaces.

Specifying code pages for phrased text search of Thai language content

Review the special instructions if you want to use phrased text search of Thai language content.

When you do a text search of Thai language content, you can perform one-word searches or phrased searches. A phrased search is several Thai words written together without spaces.

To support phrased searches in Thai content in IBM Content Manager, create the DB2 database in the Thai code page. Then create the text index in the Thai code page with the language specified as `TH_TH`. Alternatively, create the DB2 database in Unicode and create the text index in the Thai code page `CCSID 1208`.

After the database and the text index are created, you can perform two types of text searches through DB2 Net Search Extender.

- To search for one Thai word by using the regular advanced text search syntax:

```
/MyItemView[contains-text(ICMPARTS/@TIEREF,  
" 'Thai characters' ")=1]
```

- To search for Thai phrases by using the DB2 Thai-specific advanced text search syntax:

```
/MyItemView[contains-text-db2(ICMPARTS/@TIEREF,  
\" IS ABOUT TH_TH 'Thai characters' \")=1]
```

Unexpected text search results for Thai phrases

If you receive unexpected results for text search of Thai phrases, use the DB2 advanced text search syntax to resolve the problem.

Symptom

When using the Client for Windows or the APIs to text search on Thai language phrases, unexpected results return.

Cause

The default query string that is generated by the Client for Windows for text search is in the following format:

```
/MyItemView[contains-text(ICMPARTS/@TIEREF,  
" 'Thai characters' ")=1]
```

This is the basic search syntax, and only supports searching on one Thai word at a time.

To support text searching on phrases for the Thai language, use the advanced search syntax for DB2, which enables IBM Content Manager to pass the syntax directly to DB2. Add the DB2 Net Search Extender's "IS ABOUT *language word or phrase*" functionality into your query string.

Action

Modify your query string to take advantage of the advanced DB2 text search syntax for searching Thai phrases (more than one word with no spaces in between):

```
/MyItemView[contains-text-db2(ICMPARTS/@TIEREF,  
\" IS ABOUT TH_TH 'Thai characters' \")=1]"
```

If you are using the Client for Windows, use the advanced text search option to specify 'IS ABOUT TH_TH' in the optional parameters box before searching.

SQL0302N error when creating or updating a document

If you receive the SQL0302N error when creating or updating a document, you might need to increase the size limit.

Symptom

Error SQL0302N is returned during a call to create or update an item or document:

SQL0302N The value of a host variable in the EXECUTE or OPEN statement is too large for its corresponding use.

Possible cause

The BLOB or CLOB size in the following DB2 stored procedure definitions is 320 KB:

- ICMCREATEITEMS
- ICMCREATEDOCPART
- ICMUPDATEITEMS
- ICMUPDATEDOCPART

The size of the item information (total attribute size plus additional header information) cannot exceed 320 KB. If this limit is exceeded while creating or updating an item or document, error SQL0302N displays.

Action

To increase the limit, the appropriate stored procedure must be manually dropped and recreated with a larger limit. A good estimate for the appropriate limit is the total size of the item attributes plus an additional 100 KB for header information.

Execute the appropriate DB2 commands, depending on when the error occurs. This example uses 5 MB as the new limit.

For errors during create/update item

```
DROP PROCEDURE ICMCREATEITEMS;
CREATE PROCEDURE ICMCREATEITEMS
(
  OUT      lRC          INTEGER,
  OUT      lReason      INTEGER,
  OUT      lExtRC       INTEGER,
  OUT      lExtReason    INTEGER,
  IN       sTraceLevel  SMALLINT,
  IN       lReserved1   INTEGER,
  IN       szUserInfo   VARCHAR(254),
  IN       szUserToken  CHAR(32),
  INOUT    lReserved   INTEGER,
  IN       lLibraryID   INTEGER,
  IN       sNumOfItems  SMALLINT,
  INOUT    ItemCLOB     CLOB(5M),
  INOUT    ItemBLOB     BLOB(5M),
  INOUT    szItemReqNum SMALLINT,
  IN       sTran        SMALLINT,
  INOUT    szTranID     CHAR(26),
  OUT      szTranToken  VARCHAR(254)
)
DYNAMIC RESULT SETS 0
LANGUAGE C
PARAMETER STYLE DB2SQL
NO DBINFO
FENCED
PROGRAM TYPE SUB
EXTERNAL NAME 'ICMNLSSP!ICMcreate_Items';

DROP PROCEDURE ICMUPDATEITEMS;
CREATE PROCEDURE ICMUPDATEITEMS
(
  OUT      lRC          INTEGER,
  OUT      lReason      INTEGER,
  OUT      lExtRC       INTEGER,
  OUT      lExtReason    INTEGER,
  IN       sTraceLevel  SMALLINT,
  IN       lReserved1   INTEGER,
  IN       szUserInfo   VARCHAR(254),
  IN       szUserToken  CHAR(32),
  INOUT    lReserved   INTEGER,
  IN       lLibraryID   INTEGER,
  IN       sNumOfItems  SMALLINT,
  INOUT    ItemCLOB     CLOB(5M),
  INOUT    ItemBLOB     BLOB(5M),
  INOUT    sItemReqNum  SMALLINT,
  IN       sTran        SMALLINT,
  INOUT    szTranID     CHAR(26),
  OUT      szTranToken  VARCHAR(254)
)
DYNAMIC RESULT SETS 0
LANGUAGE C
PARAMETER STYLE DB2SQL
NO DBINFO
```

```

FENCED
PROGRAM TYPE SUB
EXTERNAL NAME 'ICMNLSSP!ICMupdate_Items';

```

For errors during create/update document

```

DROP PROCEDURE ICMCREATEDOCPART;
CREATE PROCEDURE ICMCREATEDOCPART
(
    OUT      lRC              INTEGER,
    OUT      lReason          INTEGER,
    OUT      lExtRC           INTEGER,
    OUT      lExtReason       INTEGER,
    IN       sTraceLevel     SMALLINT,
    IN       lReserved1       INTEGER,
    IN       szUserInfo       VARCHAR(254),
    IN       szUserToken      CHAR(32),
    INOUT    lReserved        INTEGER,
    In       lLibraryID       INTEGER,
    In       sNumOfItems      SMALLINT,
    InOut    ItemCLOB         CLOB(5M),
    InOut    ItemBLOB         BLOB(5M),
    InOut    szItemReqNum     SMALLINT,
    In       sTran            SMALLINT,
    InOut    szTranID         CHAR(26),
    Out      szTranToken      VARCHAR(254)
)
DYNAMIC RESULT SETS 0
LANGUAGE C
PARAMETER STYLE DB2SQL
NO DBINFO
FENCED
PROGRAM TYPE SUB
EXTERNAL NAME 'ICMNLSSP!ICMcreate_DocPart';

DROP PROCEDURE ICMUPDATEDOCPART;
CREATE PROCEDURE ICMUPDATEDOCPART
(
    OUT      lRC              INTEGER,
    OUT      lReason          INTEGER,
    OUT      lExtRC           INTEGER,
    OUT      lExtReason       INTEGER,
    IN       sTraceLevel     SMALLINT,
    IN       lReserved1       INTEGER,
    IN       szUserInfo       VARCHAR(254),
    IN       szUserToken      CHAR(32),
    INOUT    lReserved        INTEGER,
    In       lLibraryID       INTEGER,
    In       sNumOfItems      SMALLINT,
    InOut    ItemCLOB         CLOB(5M),
    InOut    ItemBLOB         BLOB(5M),
    InOut    sItemReqNum     SMALLINT,
    In       sTran            SMALLINT,
    InOut    szTranID         CHAR(26),
    Out      szTranToken      VARCHAR(254)
)
DYNAMIC RESULT SETS 0
LANGUAGE C
PARAMETER STYLE DB2SQL
NO DBINFO
FENCED
PROGRAM TYPE SUB
EXTERNAL NAME 'ICMNLSSP!ICMupdate_DocPart';

```

Table space is in check pending state after adding or editing a foreign key on z/OS only

You receive SQLCode 162 when adding a foreign key to an existing component type table.

Symptom

When querying or retrieving items or importing new items, the library server returns [LS RC = 7015, SQL RC = -904]

DGL5050A: SQL error executing query. XQPE query: /ITA[@SEMANTICTYPE BETWEEN 1 AND 2].

Return code: 7015. Reason code: 0. Extended return code: -904.

Extended reason code: 0.

(STATE) : [LS RC = 7015, SQL RC = -904]

There is also a warning in the library server log:

```
< DSNT404I SQLCODE = 162, SQLSTATE = >  
ICMPLSCP handleForeignKeys 06174 03/09 06:25:24.457 GMT  
;09045111471478 16:10285a68c22:X7ea2 IFVTE WARNING--  
Please perform CHECK DATA command on zOS.
```

Possible Cause

When adding a foreign key to an existing component type table (ICMUTnnnnnnsss), SQLCode 162 is returned. DB2 places a table space into CHECK PENDING state if:

1. Any table in that table space has ever been populated at any time.
2. A foreign key is added or modified for any table in the table space.

The library server performs and commits the foreign key creation. However, a warning message is written to the library server log. The message reminds you to run the CHECK DATA DB2 utility so that tables and views in this table space can be accessed.

Action

Perform the CHECK DATA command: `CHECK DATA TABLESPACE DATABASE NAME
TABLESPACE NAME`

Additional information

DB2 messages:

SQLCode 162

+162 TABLESPACE *database-name.tablespace-name* HAS BEEN PLACED IN
CHECK PENDING

Explanation: The indicated table space is in check pending status. This status exists because the ALTER TABLE statement was used to specify a referential constraint or a check constraint (while special register CURRENT RULES = 'DB2') on a populated table. The table space is not generally available until the check pending status is removed from the table space.

System Action: The table space was placed in check pending status.

Programmer Response: Run the CHECK DATA utility. The enforcement of the referential constraint or the check constraint is deferred until the CHECK DATA utility is run.

SQLCode -904

-904 UNSUCCESSFUL EXECUTION CAUSED BY AN UNAVAILABLE RESOURCE. REASON *reason-code*, TYPE OF RESOURCE *resource-type*, AND RESOURCE NAME *reason-name*

Explanation: The SQL statement could not be executed because resource *resource-name* of type *resource-type* was not available at the time for the reason indicated by *reason-code*.

Error loading libraries in a 64-bit environment

Errors that result when loading libraries in a 64-bit environment might be normal behavior.

Symptom

Messages in db2diag.log indicate failure loading libraries when the library server is running in a 64-bit environment. A typical message is like one of the following examples:

AIX

```
errno 8 loading module: /home/db2inst1/sqllib/function/ICMNLSSP(shr_64.o)
0x000000011003B420 : 0930 3530 392D 3032 3220 4361 6E6E 6F74      .0509-022 Cannot
0x000000011003B430 : 206C 6F61 6420 6D6F 6475 6C65 202F 686F      load module /ho
0x000000011003B440 : 6D65 2F64 6232 696E 7374 312F 7371 6C6C      me/db2inst1/sql
0x000000011003B450 : 6962 2F66 756E 6374 696F 6E2F 4943 4D4E      ib/function/ICMN
0x000000011003B460 : 4C53 5350 2E0A 0930 3530 392D 3132 3420      LSSP...0509-124
0x000000011003B470 : 5468 6520 7072 6F67 7261 6D20 6973 2061      The program is a
0x000000011003B480 : 2064 6973 636F 6E74 696E 7565 6420 3634      discontinued 64
0x000000011003B490 : 2D62 6974 206F 626A 6563 7420 6669 6C65      -bit object file
0x000000011003B4A0 : 2E                                     .
```

Solaris

```
2005-12-21-08.46.08.180075-480 E807A594          LEVEL: Error (OS)
PID      : 11859          TID : 1          PROC : db2fmp (3906) 0
INSTANCE: db2inst2      NODE : 000
FUNCTION: DB2 UDB, oper system services, sqloLoadModule, probe:190
CALLED   : OS, -, dlopen
OSERR    : EBADF (9) "Bad file number"
DATA #1 : Library name or path, 46 bytes
/export/home/db2inst2/sqllib/function/ICMNLSSP
DATA #2 : shared library load flags, PD_TYPE_LOAD_FLAGS, 4 bytes
0
DATA #3 : String, 99 bytes
ld.so.1: db2fmp: fatal: /export/home/db2inst2/sqllib/function/ICMNLSSP:
wrong ELF class: ELFCLASS32
2005-12-21-08.46.09.318712-480 I1402A416          LEVEL: Warning
PID      : 11859          TID : 1          PROC : db2fmp (3906) 0
INSTANCE: db2inst2      NODE : 000
MESSAGE  : sqlerRoutineLoad (-444): input string ...
DATA #1 : Hexdump, 26 bytes
0x000000010025E8CA : 4943 4D4E 4C53 5350 2149 434D 6C69 7374      ICMNLSSP!ICMlist
0x000000010025E8DA : 5F4E 4C53 4B65 7977 7264                      _NLSKeywrd
```

Possible Cause

The stored procedures, ICMNLSSP, ICMNLSUF, and ICMNWFSP, are 32-bit libraries. In a 64-bit environment, DB2 tries first to load them in a 64-bit fenced-mode process. When this attempt fails, DB2 loads them in a 32-bit fenced-mode process. The indication of the initial failure is recorded in the db2diag.log file.

Action

This behavior is normal behavior. Monitor your log file size to make sure that the file system does not fill up because of extra messages. No other action is necessary.

DGL0394A error when trying to log on to the library server with the system administration client

Review the node and database settings if you receive the DGL0394A error when you are trying to log on to the library server.

Symptom

When attempting to connect to an IBM Content Manager server with the system administration client, you receive a DGL0394A error: SQL1336N: The remote host was not found.

Cause

The DB2 Universal Database node and database for the library server database might not be cataloged correctly.

Action

From a DB2 command prompt, verify the node and database settings:

```
DB2 LIST NODE DIRECTORY
```

```
DB2 LIST DATABASE DIRECTORY
```

Here are sample commands for defining the node and database:

```
DB2 CATALOG TCPIP NODE mylsnode REMOTE  
      server1.abc.com SERVER 50000
```

```
DB2 CATALOG DATABASE icmn1sdb AS mylsdb AT NODE  
mylsnode
```

Tip: In the sample, there should be a matching ICMSEVER=MYLSDB entry in the cmbicmsrvs.ini file.

You can also use the DB2 Universal Database Client Configuration Assistant to define the node and database.

Error LS RC 7017 SQL RC -670 row length exceeded limit

You receive a database error when you try to add attributes to an item type.

Symptom

When attempting to add attributes to an existing item type, you receive this error: SQL0670N The row length of the table exceeded a limit of "32677" bytes.

Cause

The error is returned from the DB2 database where the library server resides. The row length of the table corresponding to the item type has exceeded the limit of the maximum 32 KB size of the table space ICMLFQ32. The row length of the table includes the size of both the user-defined attributes and the library server system columns.

Action

If the row length of a table is greater than 32 KB, use BLOB or CLOB attributes for the new attributes. Use these types of attributes because the length of these two attribute types is not counted as part of the row length used for the buffer pool.

Insufficient space when creating a large number of item types and item type subsets

If you receive an insufficient space error when you create many entities, you can take several actions to correct the problem.

Symptom

When creating more than 1300 item types and 3000 item type subsets, this error displays:

```
JVMST109: Insufficient space in Javaheap  
to satisfy allocation request.  
Exception in thread "main" java.lang.OutOfMemoryError.
```

Cause

The client application does not have the memory to create and cache the total number of entities (item types and subsets). The IBM Content Manager server components and database function without error.

Action

You can create more entities with these actions:

1. Increase the Java Virtual Machine (JVM) heap size when you are running your application. Enter:

```
java -Xms256M -Xmx2304M javaClass
```
2. Scale the application by using multiple JVM machines to run the application.

You can use the same workaround to handle creating large numbers of users, user groups, access control lists (ACLs), work nodes, and document routing processes.

Changing the host name the resource manager uses to communicate with the library server

If the library server host name changes, you must update the server definition in the resource manager.

Symptom

The resource manager and library server are on different machines and cannot communicate when the host name of the library server is changed.

Action

You can use the system administration client to change the host name that the resource manager uses to communicate with the library server. Perform these steps:

1. Click your resource manager in the system administration client. Click **Server Definitions > ICMNLSDB > Properties**.

2. Change the library server host name.

The host name is also stored on the library server in the *IBMCMROOT\config\ibmcmcfg.params* file. The HOSTNAME entries in this file are used for various purposes on different operating systems. Update them as needed if a host name changes.

SQL error code -181: Asynchronous recovery process cannot delete the entries in ICMSTItemsToDelete table

The asynchronous recovery process might fail if different date or time formats are used on the library server and resource manager.

Symptom

When a user uses an application to delete an item, it is deleted internally from the library server. The related objects on the resource manager are either marked or physically deleted from resource manager. The ICMSTItemsToDelete table identifies the items on the resource manager that are marked for future deletion by the asynchronous recovery process. In this case, the entries in the table become larger and larger over time and the objects marked for deletion cannot be deleted from the resource manager. Error messages are produced in the library server log, *icmsserver.log*, when this problem happens.

Cause

The asynchronous process calls the library server store procedure to access ICMSTItemsToDelete and to delete the related objects periodically. In this case, the library server finds that the timestamp passed in the *cleanup_ToBeDelTable* routine was invalid and fails in decoding the time stamp from the resource manager. This problem happens because different date and time formats are used on the library server and resource manager databases.

Action

Include the following line in the *db2cli.ini* file on the resource manager machine. This line controls the date format used by DB2:

```
[COMMON]
DateTimeStringFormat=ISO
```

Implementing this change in the [COMMON] section of the *db2cli.ini* file requires significant testing, because the change affects all applications using DB2 on the server.

The alternative action is to make the change to a specific database. You can limit the impact to a specific database by using the following command:

```
[CMSpecificAlias]
DateTimeStringFormat=ISO
```

where *CMSpecificAlias* is the database name.

Transaction log file for the database is full

If you receive errors about the transaction log for the database being full, you might need to increase the log file size and the number of primary and secondary log files.

Symptom

This error message displays:

```
[IBM][CLI Driver][DB2/NT] SQL0964C The transaction log for the
database is full.  SQLSTATE=57011
```

Cause

This message is usually caused when the database log file is not large enough for the application or the application is not updating transactions often enough to prevent the transaction log from becoming full.

Action

1. To obtain the DB2 log file configuration, from a DB2 command prompt, run:

```
db2 get db cfg for database name
```

The output related to the log file is displayed. This sample output shows that the database uses five log files, three for primary and two for secondary, respectively. Each file is 1 MB (250 x 4 KB) in size:

Log file size (4KB)	(LOGFILSIZ) = 250
Number of primary log files	(LOGPRIMARY) = 3
Number of secondary log files	(LOGSECOND) = 2

2. Increase LOGFILSIZ, LOGPRIMARY, and LOGSECOND. For example, enter:

```
db2 update db cfg for database name using
logfilsiz 1000 logprimary 20 logsecond 10
```

The DB2 command updates the log file size to 4 MB (1000 x 4 KB) in size with 20 primary log files and 10 secondary log files.

3. Restart DB2 using **db2stop** and **db2start**.

DGL0394A error when connecting to an IBM Content Manager server using the system administration client

If a user cannot connect remotely by using the system administration client, some parameters in the cmbicmsrvs.ini file might be incorrect.

Symptom

A user can connect remotely to IBM Content Manager with icmadmin and icmconct from a DB2 command line. However, the user cannot log on remotely using the system administration client:

```
DGL0394A: Error in ::DriverManager.getConnection;
[IBM][CLI Driver]
CLI0124E Invalid argument value. SQLSTATE=HY009
(STATE) : ; [SERVER =
YoumansECM, USERID = icmconct, SQL RC = -99999,
SQL STATE = HY009]
```

Cause

The cmbicmsrvs.ini file, which contains a list of all of the available IBM Content Manager library servers on the client machine, has incorrect parameters.

Action

Ensure that the parameters in cmbicmsrvs.ini are correct. The parameters are all case sensitive. Follow these steps:

1. Catalog the remote database.
2. Find the CMCOMMON directory containing .ini files. The directory is identified by the CMCOMMON environment variable. The default location is Program Files\IBM\CMGMT on Windows.
3. Open the cmbicmsrvrs.ini file.
4. Copy the entire first block of information starting with ICMSERVER and ending with ICMOSTYPE.
5. Paste the block as a separate block after the first block, leaving a space between it and any other blocks of text.
6. Modify the variables as needed. Typically, you only need to change ICMSERVER from ICMNLSDB to the name of the remote database that you cataloged.
7. Save and then connect using the name of the remote database. In the system administration client, you should see the remote databases in the list of servers to which you can connect.

Troubleshooting batch load utility problems for Content Manager for z/OS

Problems with the batch load utility for Content Manager for z/OS might include invalid parameters, invalid credentials, or inconsistent data in the input files.

This section describes how to troubleshoot common problems with the high-volume batch load utility for Content Manager for z/OS.

“Receiving ICMBL010E error message when running a generated batch load program”

“Receiving ICMBL023E error message when running a generated batch load program” on page 624

“Receiving ICMBL024E error message when running a generated batch load program” on page 624

“Receiving ICMBL001E and ICMBL002E error messages when running a generated batch load program” on page 625

Receiving ICMBL010E error message when running a generated batch load program

A high volume batch load utility error ICMBL010E might be related to invalid parameters in the CTLDATA file.

Symptoms

You submitted the ICMMBLJ1 job to run a generated batch load program, but it failed with error message ICMBL010E.

Causes

The CTLDATA input file specified on the job contains one or more invalid parameters.

Resolving the problem

Correct the parameters and values specified in the CTLDATA file, then run the ICMMBLJ1 job again.

User response: For more information, consult the information provided in the SYSPRINT output data set.

Receiving ICMBL023E error message when running a generated batch load program

A high volume batch load utility error ICMBL023E might be related to invalid data in the IDXDATA file.

Symptoms

You submitted the ICMMBLJ1 job to run a generated batch load program, but it failed with error message ICMBL023E.

Causes

The IDXDATA input file specified on the job contains invalid data.

Resolving the problem

Correct the columns and values defined in the IDXDATA file, verifying the size and user attribute data of the objects to be loaded, then run the ICMMBLJ1 job again.

User response: For more information, consult the information provided in the SYSPRINT output data set.

Receiving ICMBL024E error message when running a generated batch load program

A high volume batch load utility error ICMBL024E might be related to inconsistent data in the IDXDATA and OBJDATA input files.

Symptoms

You submitted the ICMMBLJ1 job to run a generated batch load program, but it failed with error message ICMBL024E.

Causes

The data defined in the IDXDATA and OBJDATA input files do not correlate correctly. The batch load program uses the record length specified in the IDXDATA file to retrieve the corresponding object data from the OBJDATA file. The batch load program then advances to the end of the current object to begin retrieval for the next object that is defined. If any record length specified in the IDXDATA file is not correct, the batch load program might run out of object data before reaching the end of the IDXDATA file.

Diagnosing the problem

Compare the data in the IDXDATA and OBJDATA files, looking for inconsistencies between the data's actual length in the OBJDATA file and the record length specified in the IDXDATA file.

Resolving the problem

Correct the column data and metadata specifications in the IDXDATA and OBJDATA files, then run the ICMMBLJ1 job again.

User response: For more information, consult the information provided in the SYSPRINT output data set.

Receiving ICMBL001E and ICMBL002E error messages when running a generated batch load program

High volume batch load utility errors ICMBL001E and ICMBL002E might be related to incorrect privileges.

Symptoms

You submitted the ICMMBLJ1 job to run a generated batch load program, but it failed with error messages ICMBL001E and ICMBL002E.

Causes

The user ID running the ICMMBLJ1 job was not defined with the ClientImport privilege.

Resolving the problem

Use the system administration client to define the user ID with the ClientImport privilege in the IBM Content Manager library server, then run the ICMMBLJ1 job again.

User response: For more information, consult the information provided in the SYSPRINT output data set.

Troubleshooting the XML schema mapping tool

Problems with the XML schema mapping tool can be related to item type imports and indexing failures.

This section provides troubleshooting assistance for the XML schema mapping tool.

“Troubleshooting XML schema mapping tool errors”

“Unable to import item types with the entityView property specified in the annotation dialog box using the XML schema mapping tool” on page 626

“Locating an object that did not get indexed” on page 216

Troubleshooting XML schema mapping tool errors

When errors occur in the XML schema mapping tool, you can check for more information in the connection layer log or on the console.

Symptom

Cannot locate information when errors occur in the XML schema mapping tool.

Possible Cause

Errors can occur for many reasons.

Action

Frequently, errors occur in the IBM Content Manager connection layer. A record of these errors can be found in your working directory in log/connectors/userid.dklog.log.

Because some errors might not be logged by the connector, the XML schema mapping tool also displays error information on the console. This information can be captured and placed in a text file for later review, or sent to IBM Software Support for evaluation.

On Windows, the console is normally hidden; therefore, users do not see this output. To see the console, open a Windows command prompt window and start the tool using the command: "%IBMCMROOT%\admin\common\cmxmlmap81.bat" server userid password.

The console remains open when the tool is used and displays error information if appropriate.

Unable to import item types with the entityView property specified in the annotation dialog box using the XML schema mapping tool

You must use a specific procedure to import item types with the entityView property specified in the annotation of the XML schema.

Symptom

When you are trying to import an item type with the entityView property specified in the annotation of the XML schema of the item type, a DKXMLException with error code DGL0638 displays.

Cause

The XML schema mapping tool was not designed to support creating a view rather than an item type. It validates that component names are unique and that attributes match the attributes that are already defined to the library server. If not, it gives them a new name and creates them. This behavior causes the view creation to fail.

Action

To create a view to an item type in the XML schema mapping tool, and map in to it by making sure that the attributes match, follow these steps:

1. Use the system administration client to export the item type to a file.
2. In the XML schema mapping tool, load the source schema, and then load the target schema from the file that was created.
3. Remove all annotations from the target schema.
4. For the root and any child components, add only the entityView annotation property setting, baseEntityType, to the name of the component (the item type or child component name).
5. Edit the root node and any child components, changing the name property to something unique.
6. Remove any attributes that you do not want in the view.
7. Create the mapping and generate and test the query, and save.
8. Select import as **Content Manager item type** on the target tree node. Give it the same name as the root node.
9. Use the system administration client to verify the view creation and set additional properties such as display names, attribute access, and filter.

Locating an object that did not get indexed

When text indexing ends abruptly, the document that was being indexed does not get indexed, so you must locate and reindex that document.

To find the document, or object, complete the following steps:

1. In a DB2 command window, run the following command:

```
db2 "select EVENTVIEWSHEMA, EVENTVIEWNAME from
DB2EXT.TEXTINDEXES where INDSHEMA = 'ICMADMIN' and INDNAME =
'ICMUT01001001TIE'"
```

Where the text index name is ICMUT01001001TIE and the schema is ICMADMIN.

You receive a list of event views. Each event view has a column named MESSAGE. This column contains the message text corresponding to an error or SQL warning and SQL state that is returned by the ICMFetchFilter UDF.

2. Use the item ID and version ID to locate the document that did not get indexed in your system.

Example

Example SQL state warning returned by the UDF:

```
CTE0100 A DB2 operation failed. DB2 information: "01H20"
"[IBM][CLI Driver][DB2/6000] SQL0462W Routine "ICMFETCHFILTER"
(specific name "") has returned a warning SQLSTATE, with diagnostic
text "A1001001A07G30B63645B75442 1 Timeout after 60 seconds".
SQLSTATE=01H20
```

The first string is the item ID of the object that caused the system to stop, timeout. The next string is the object version ID. The 01H20 warning state means that a timeout has occurred. The diagnostic text is the text the UDF returned to NSE for this type of warning. Therefore, the example message indicates that an object with item ID A1001001A07G30B63645B75442 and version ID 1 timed out after 60 seconds.

Using the item ID and version ID, you can find the TIERef string associated with the document and invoke the UDF to test if the timeout value that was set is too small or if there is a problem with the object.

Before you invoke the UDF, disable the timeout feature by using the system administration client, or by running the following DB2 command:

```
db2 update ICMSTSYSCONTROL set UDFTIMEOUT=0
```

You can also set the value to a large number, such as 36000 seconds (again, using the system administration client or by issuing a DB2 command).

You can then manually invoke the UDF by entering the following command:

```
db2 "values icmfetchfilter('...')"
```

where ... is the TIEREF string from the previous step. The text data from the object should be returned.

Troubleshooting the resource manager

Problems with the resource manager can involve problems with other content management components and other prerequisite products. For example, troubleshooting a problem with the resource manager can also include troubleshooting steps on the library server or Web server.

This section describes how to troubleshoot common resource manager problems.

The resource manager contains information about the storage of objects. The resource manager is a Web application, and the troubleshooting approach to the resource manager is different than the approach required to troubleshoot the library server.

Configuration errors with IBM HTTP Server, DB2, or either WebSphere Business Integration Server Foundation or WebSphere Application Server can cause resource manager failures. You must be able to locate the failing product, and know how to correct the problem to maintain a resource manager server.

Because the resource manager is a Web application, various components are involved when handling requests. For example, when a client requests a document, the library server, Web server, and resource manager Web applications are all involved. You need the log files generated by each component involved in the request to troubleshoot resource manager problems.

The following list describes the flow of a request from a client to a resource manager:

1. A client must first obtain a token from the library server. After the client obtains the token, the client can reuse it until the token expires. (You define the token duration on the Resource Manager Properties window in the system administration client.)
2. The client passes its request and this token to the HTTP Server.
3. The WebSphere Business Integration Server Foundation or WebSphere Application Server plug-in (running on the HTTP Server) forwards the request to the resource manager Web application, which runs on WebSphere Business Integration Server Foundation or WebSphere Application Server.
4. The resource manager web application first validates the token.
5. Depending on the type of request made by the client, information is read from, or stored in, the resource manager database (called RMDB by default) and file system volume (or drive C on Windows servers).

“Retrieving large objects from the resource manager” on page 629

“DB2 SORT errors in resource manager” on page 629

“System failed to create new Tivoli Storage Manager volume” on page 630

“No suitable driver in the log file when starting the resource manager for IBM Content Manager with DB2 Universal Database” on page 631

“Verifying database creation and deployment” on page 632

“Troubleshooting resource manager database creation errors using the icmcrmdb.log” on page 632

“Verifying resource manager deployment” on page 633

“Verifying database connections” on page 634

“Verifying communication with the Web server” on page 634

“Secure Sockets Layer” on page 635

“Resource manager is not online or available” on page 635
“Error storing objects in Object Access Method (OAM)” on page 637
“Changing the resource manager port number on UNIX and Windows” on page 637
“Changing the resource manager port number on z/OS” on page 638
“Manually synchronizing the encryption key” on page 639
“DB2 return code -818 during SMS interface utility processing” on page 640
“Deadlock error SQL0911 RC=2 when importing documents or replicating to a target resource manager” on page 641
“Error message ICM9712 failed to store documents” on page 641
“Enabling the advertisement of byte serving capability for document retrieval to the clients” on page 642
“Troubleshooting resource manager asynchronous jobs” on page 643
“Troubleshooting database connection failures on the resource manager” on page 645

Retrieving large objects from the resource manager

A problem with retrieving large objects from the resource manager might be related to the value set for the `channelwritetype` parameter.

Symptom

You receive an `OutOfMemory javacore` dump error when attempting to retrieve a large object, such as 1.9 GB file.

Cause

The parameter `channelwritetype` must be set to `sync`.

Action

1. In the WebSphere Application Server Administration Console, go to **Servers > Application servers > serverName > Web Container Settings > Web Container > Custom Properties** and click **New**.
2. In the **Name** field, enter `com.ibm.ws.webcontainer.channelwritetype`.
3. In the **Value** field, enter `sync`.
4. Click **OK** and then **Save** to save the configuration.

DB2 SORT errors in resource manager

Sort errors in the resource manager can be related to the value set for the `SORTHEAP` database configuration variable.

Symptom

An `SQL0955C` error is displayed related to DB2 SORT errors in the resource manager.

Action

Update the database configuration variable, `SORTHEAP`, using the following update command. The default heapsize for sort is 256 pages, a size that is

equivalent to 1 MB (with each page as 4 KB). Depending on your application, you can add more pages to it, but do not add more than the sort threshold size for the instance (SHEAPTHRES).

1. Get the instance sort threshold and database heap size for sort, where *rmdb* is the name of your resource manager.

```
db2 get dbm cfg | grep SHEAPTHRES
db2 get db cfg for rmdb | grep SORTHEAP
```

2. Update sort size to 2 MB:

```
db2 update db cfg for RMDB using SORTHEAP 512
```

System failed to create new Tivoli Storage Manager volume

If the system fails to create a Tivoli Storage Manager volume, there might be a missing DLL file in the path.

Symptom

UnsatisfiedLinkError error when defining a new Tivoli Storage Manager volume.

The following type of error message appears in the *icrmr.logfile* log file:

```
java.lang.UnsatisfiedLinkError:
C:/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/libraNode01Cell/
icrmr.ear/icrmr.war/lib/windows/DMAeJAdsmApi.dll (JVMPORT015E
Unable to resolve DLL references - a prerequisite DLL may be missing).
```

Possible cause

A prerequisite DLL of the *DMAeJAdsmApi.dll* file might be missing.

Action

Identify the missing DLL and add it to %PATH% (or \$LIBPATH), then restart the resource manager.

Attention: On a Linux system, you might need to download and install the Intel library on your system.

Example

The following example is for the Windows platform:

The Depends tool scans the WIN module to find all dependent modules. In the following example, *TSMAPI.dll* is a dependent module for *DMAeJAdsmApi.dll*. In this example, the solution is to add the path of *TSMAPI.dll* to %PATH% so that *DMAeJAdsmApi.dll* can find it. *TSMAPI.dll* was located in *\$TSM_HOME\api\DLL*. A typical path looks like *c:\IBM\Tivoli\TSM\api\DLL*.

```
C:\ibm\WebSphere.6.1\AppServer\profiles\appSvr01\installedApps\
libraNode01Cell\icrmr.ear\icrmr.war\lib\windows> depends
DMAeJAdsmApi.dll
```

```
ntdll.dll
```

```
KERNEL32.dll
```

```
DMAeJAdsmApi.dll
```

Not found: TSMAPI.dll

No suitable driver in the log file when starting the resource manager for IBM Content Manager with DB2 Universal Database

A "no suitable driver" error in the resource manager log file might be related to JDBC driver initialization.

Symptom

When you are starting the resource manager, there are multiple errors in the resource manager log file, `icrmr.logfile`. The first of these errors is like this one:

```
ICMRM:ERROR 2005-07-23 03:48:13.017000 context:
[P=485758:0=0:CT]
- ICM9832: SQL Error: 0, SQLMsg: No suitable
driver SQLState: 08001 - createPool
(ICMRMConnectionPoolManager.java:309)
java.sql.SQLException: No suitable driver
at java.sql.DriverManager.getConnection(DriverManager.java:559)
at java.sql.DriverManager.getConnection(DriverManager.java:189)
at com.ibm.mm.icrmr.ICMRMConnectionPoolManager.createPool
(ICMRMConnectionPoolManager.java:274)
at com.ibm.mm.icrmr.ICMRMConnectionPoolManager.createPool
(ICMRMConnectionPoolManager.java:251)
at com.ibm.mm.icrmr.ICMRMConnectionPoolManager.
(ICMRMConnectionPoolManager.java:185)
at com.ibm.mm.icrmr.ICMRMConnectionPoolManager.
(ICMRMConnectionPoolManager.java:81)
at com.ibm.mm.icrmr.ICMResourceManager.init
(ICMResourceManager.java:412)
```

Possible Cause

The JDBC driver is not initialized properly. The library path and the DB2INSTANCE environment variables are not set. The usual reason for this problem is that the DB2 Universal Database instance profile is not set or the environment has changed, perhaps because of a **su** or **sudo** command. The library path (LIBPATH on AIX and LD_LIBRARY_PATH on Solaris and Linux) is often not transferred for reasons of security when calling the **sudo** or **su** command.

Action

Directly source the DB2 instance profile each time before starting the resource manager server.

For example, if the `db2inst1` variable is the db2 instance and the `icrmr` variable is the resource manager server name, enter the appropriate commands:

```
AIX    . /home/db2inst1/sqllib/db2profile /usr/WebSphere/AppServer/bin/
startServer.sh icrmr
```

```
Linux  . /home/db2inst1/sqllib/db2profile /opt/WebSphere/AppServer/bin/
startServer.sh icrmr
```

Solaris

```
. /export/home/db2inst1/sqllib/db2profile /opt/WebSphere/AppServer/
bin/startServer.sh icrmr
```

Verifying database creation and deployment

If you or your users have problems with the resource manager, verify that the database was created and deployed successfully.

To verify that the database was created and deployed successfully:

1. On the server where you installed the resource manager database, enter the following command at a DB2 command prompt:

```
list db directory
```

Verify that the resource manager database name appears in the list of databases.

- If the resource manager is listed, continue with step 2.
- If it is not listed, see “Troubleshooting resource manager database creation errors using the icmcrrmdb.log.”

2. At the same command prompt, enter:

```
connect to resourcemanager_dbname user userID using password
```

- If the connection succeeds, continue with step 3.
- If the connection fails, see “Troubleshooting resource manager database creation errors using the icmcrrmdb.log.”

3. At the same command prompt, enter:

```
list tables
```

Verify that the program returns a list of approximately 25 tables.

- If the system displays the expected number of tables, continue with step 4.
- If the system displays fewer tables, see “Troubleshooting resource manager database creation errors using the icmcrrmdb.log.”

4. Verify that the resource manager was deployed and is started. Enter:

```
list applications
```

When the resource manager starts, it attempts three connections to the resource manager database. Verify that the program displays three `java.exe` applications, and that the resource manager name is listed in the **DB Name** column. If you receive results that are different from those results, see “Verifying resource manager deployment” on page 633 and “Verifying database connections” on page 634.

Troubleshooting resource manager database creation errors using the icmcrrmdb.log

You can use the error messages that are returned in the installation log file to fix resource manager database creation problems.

To use the installation log file to fix resource manager database creation problems:

1. Open the resource manager installation log, the `icmcrrmdb.log` file. This file is located in the `IBMCMROOT` path.
2. Read the `icmcrrmdb.log` file carefully to verify that all SQL commands completed successfully. You must distinguish between error and warning messages, because the `icmcrrmdb.log` file contains both.
3. Correct any errors described in the `icmcrrmdb.log` file.

Tip: A common error when creating the resource manager database is forgetting to grant the required DB2 administration (`db2admin`) privileges to the resource manager user ID (usually `rmadmin`). This situation is reflected in the following message:

RADMIN does not have the privilege to perform operation.

4. If the error messages indicate that the resource manager was never created, or was created with zero tables, create a resource manager database using the resource manager creation utility.
 - On UNIX servers, launch the resource manager creation utility, `icmcreatermdb.sh`, from a command prompt.
 - On Windows servers, launch the command-line utility by clicking: **Start > Programs > IBM Content Manager Enterprise Edition > Resource Manager Database Install**.

Requirement: To create the resource manager database on any server, you must be logged in with a user ID that has db2admin privileges. In some configurations, you might need to log in to a server with a user ID that does not have db2admin authority. In that case, you must switch to a new user ID with the appropriate db2admin privileges before running the resource manager database creation utility.

5. Verify the new resource manager by following the steps in “Verifying database creation and deployment” on page 632.

Verifying resource manager deployment

Many problems with resource manager deployment are related to problems with the deployment of the Web application.

When troubleshooting a resource manager problem, it is important to verify that the resource manager Web application was successfully deployed during installation. If the Web application was not installed properly, or if the Web server plug-in was not regenerated, then the resource manager server cannot respond to client requests or perform other tasks.

A client accesses the resource manager in one of the following ways:

- Through the Web server (typically IBM HTTP Server), and a request to port 80 by `http://server/icmrm/snoop`. The Web server plug-in forwards the request to WebSphere Business Integration Server Foundation or WebSphere Application Server.
- Directly to WebSphere Business Integration Server Foundation or WebSphere Application Server by specifying the port that the application server instance is listening on: `http://server:port/icmrm/snoop`. Substitute the actual port number for *port*.

To test the direct-access method, open a browser and enter the following address: `http://server:port/icmrm/snoop`. Substitute the actual port number for *port*. If you receive a failure notice, then either the resource manager Web application is not started, or the resource manager was improperly deployed.

You can try to manually deploy or start the resource manager Web application to help solve the problem. Follow the steps in the *Planning and Installing Your Content Management System* to manually deploy or start the resource manager.

The WebSphere standard error log file might also contain error messages related to the resource manager deployment and operation. The standard log file is located in the `logs` directory in the WebSphere installation path.

If the direct method succeeds, but going through the Web server (<http://server/icrm/snoop>) fails, the problem is in the Web server plug-in. Follow the steps in the *Planning and Installing Your Content Management System* to regenerate the Web server plug-in.

Retest the direct and indirect access methods.

Verifying database connections

To help troubleshoot problems with client requests, verify the connection between the Web application and resource manager database.

When the resource manager Web application starts, it attempts to make three connections to the resource manager database. If the Web application cannot connect to the resource manager database, the resource manager cannot process client requests.

The following steps explain how to validate the connection between the Web application and resource manager database.

1. If the resource manager database is on a remote server and you have not cataloged the database, either locally catalog the database or log on to the remote server where you installed the database. Whether the database is local or remote, you must log on with, or have the authority to switch to, a user ID that has db2admin privileges.
2. At a DB2 command prompt, enter
`list applications`

The system displays a table of all DB2 applications.

- If the table lists three resource manager applications, then the connections are working correctly.
- If the connections do not appear, then the resource manager Web application is having a problem connecting to the database. Usually, this problem occurs when the user ID and password used by the resource manager to connect to the database are invalid.

Tip: You can test the user ID and password that you enter here by issuing the following command from a DB2 command prompt:

```
connect to rmdb user user_id using password
```

Database connections also fail if the db2jcc.jar file is not in the WebSphere classpath. In this circumstance, the WebSphere standard error log file contains a message indicating that the DB2 JDBC driver was not found.

Verifying communication with the Web server

A problem with Web server communication might be related to an incorrect resource manager host name.

If the resource manager host name was incorrectly specified during the installation, or if the resource manager host name was changed, a client request can never reach the Web server. By default, the IBM HTTP Server logs every client request in the `access.log` file. You can use the `access.log` file to verify the resource manager Web address and that the client requests are getting to the Web server.

In the system administration client, you can define the Web address for the client to use to access the resource manager. To view the resource manager configuration, open the system administration client, select a resource manager, and click **Properties**.

Secure Sockets Layer

Problems with accessing the resource manager from the system administration client might be because of problems with Secure Sockets Layer.

Secure Sockets Layer (SSL) is required only to perform resource manager configuration. Therefore, if you are having problems importing or retrieving documents, you can conclude that SSL is not the cause. If you are trying to access the resource manager from the system administration client and you receive an error, SSL might be the cause.

1. Make sure that your resource manager is operating properly by either importing or retrieving a document.
2. Use the SSL test procedure.
3. If you are using IBM HTTP Server as your SSL manager, review `error.log` for SSL-related error messages. The log file location is determined by the `ErrorLog` directive in the IBM HTTP Server configuration file. The default log directories are:

AIX `/usr/IBMIHS/logs/error_log`

Linux `/opt/IBMIHS/logs/error_log`

Solaris
 `/opt/IBMIHS/logs/error_log`

Windows
 `server_root\logs\`

4. If you are using WebSphere Business Integration Server Foundation to manage SSL, review the log files. The default log locations are:

AIX `/usr/WebSphere/AppServer/logs`

Linux `/opt/WebSphere/AppServer/profiles/RM_PROFILE/logs`

Solaris
 `/opt/WebSphere/AppServer/logs`

Windows
 `c:\Program Files\IBM\WebSphere\AppServer\logs`

Resource manager is not online or available

If you receive a message that a running resource manager is not online or available, the resource manager might be marked offline from a previous connection failure.

Symptom

Users can import documents but not retrieve them, even though the resource manager is deployed and started. Users receive message DGL7186A:

Resource manager [RMDB] is not online and/or available

Possible cause

This error typically originates from an IBM Content Manager system that was previously in an unusual state. The error is usually caused if you run the library server monitor process before creating the resource manager instance. When the library server monitor process finds a resource manager definition in the library server but cannot connect to that resource manager, the monitor process marks the resource manager as offline.

Action

First, verify that your resource manager is marked offline. Then mark it online.

If you cannot use the system administration client to verify that the resource manager is marked offline and mark it online, you can do so manually.

1. "Verifying that a resource manager is marked offline"
2. "Marking a resource manager online"

Verifying that a resource manager is marked offline

Some maintenance tasks must be done when the resource manager is offline. Use this procedure to verify that the resource manager is offline.

To verify that a resource manager is marked as offline, complete the following steps:

1. Access the local or remote server where the library server associated with the resource manager is installed.
2. Open a DB2 command prompt and enter:
connect to lsdatabasename user userID using password
3. Enter the following DB2 command to query the resource manager definitions:
select RMCODE,RMNAME,RMFLAGS from ICMSTRESOURCEMGR
4. Verify that the output looks like the following example:

RMCODE	RMNAME	RMFLAGS
0	RESERVED	0
1	RMDB	2

2 record(s) selected.

5. In your output, look for the resource manager from which you are attempting to retrieve documents. If the resource manager RMFLAGS value is 2, then it has been marked offline.

Important: Be sure to remember the RMCODE value. You must type it when you update the library server to mark the resource manager as online.

Marking a resource manager online

For your content management system to work correctly, the resource manager must be marked as online in the library server. Use this procedure to mark a resource manager as online.

To mark a resource manager as online, update the ICMSTRESOURCEMGR value. This value is set on the library server that is associated with the resource manager.

Complete the following procedure:

1. Access the local or remote server where the library server associated with the resource manager is installed.
2. Open a DB2 command prompt and enter:
`connect to lsdatabasename user userID using password`
3. Update the resource manager definition by typing:
`update ICMSTRESOURCEMGR set RMFLAGS=0 where RMCODE=rmcode_value`

Error storing objects in Object Access Method (OAM)

Errors received when using OAM to store objects can be traced to several different problems that occur the first time that an object is stored.

Symptom

When using OAM to store objects in an IBM Content Manager resource manager on z/OS, you receive a return code 16 with reason code D8010000.

Action

If the following criteria are not met, you might receive this return code the first time that an object is stored:

- The resource manager CGI program must be program controlled in UNIX System Services (USS).
- Data set with DSNALI must be on the STEPLIB.
- All of the data sets on the STEPLIB must be APF authorized.
- The resource manager ICMMRMBD bind job and ICMMRMGT grant job must be run with the OAM packages for the applicable specified storage groups.

Changing the resource manager port number on UNIX and Windows

If you change the resource manager port number, you must remember to change it in all required locations.

Symptom

The port number for HTTP access was updated in the resource manager definition in the system administration client, but communication with the resource manager fails.

Possible cause

The port number was changed in the system administration client, but not in other places where it appears.

Actions

Attention: Port 80 can be disabled by modifying the `httpd.conf` file and removing references in WebSphere Business Integration Server Foundation or WebSphere Application Server to port 80. Port 80 is used for many Web applications, however.

Tip: The default resource manager application server is called `icrm`.

1. Update the `httpd.conf` file:

- a. Make a backup copy of the `httpd.conf` file.
 - b. Open the `httpd.conf` file in a text editor.
 - c. Add a `Listen` statement with the port you specified in the access type:
`Listen new_port_number`
 - d. Save the file and exit.
2. Update WebSphere Business Integration Server Foundation or WebSphere Application Server:
 - a. Start the WebSphere Business Integration Server Foundation or WebSphere Application Server administrative console.
 - b. Click **Environment > Virtual Hosts > Default Host > Host Aliases > New** to identify the new port. For the **Host Name** field, enter *, the IP address, the DNS host name with domain name suffix, or the DNS host name alone. For the **Port** field, enter the new port number. Apply and save the settings.
 - c. Regenerate the plug-in. Click **Environment > Update Web Server Plugin > OK**.
3. Restart the HTTP server.
4. Restart the resource manager application server.
5. Enable logging by modifying `cmblogconfig.properties` and verify that all access is taking place through the specified port.
6. To verify the configuration, perform each of the following tests in order.
 - a. In a Web browser, enter `http://hostname:new_port`. You should see the IBM HTTP Web page.

Tip: If the test fails, try pointing the browser to port 80 to verify that the new port went into effect. Open the `httpd.conf` file and make sure that the new `Listen` statement is there. Restart the IBM HTTP Server.
 - b. In the browser, enter `http://hostname:new_port/icmrm/snoop`. You should see the snoop servlet page with information about your local system.

Tip: If the test fails, make sure that the resource manager application server is started.
 - c. Use the eClient or Windows client to retrieve and store a document.

Tip: If the test fails, you must troubleshoot your resource manager. Check the `dklog.log` file for any errors. Make sure that there is a fully qualified hostname in resource manager definition in the system administration client.

Related tasks

“Viewing or modifying an access type” on page 53

Changing the resource manager port number on z/OS

If you change the resource manager port number, you must remember to change it in all required locations.

Symptom

The port number for HTTP access was updated in the resource manager definition in the system administration client, but communication with the resource manager fails.

Possible cause

The port number was changed in the system administration client, but not in other places where it appears.

Actions

1. From UNIX System Services (USS), update the `httpd.conf.port_number` file:
 - a. Make a backup copy of the `httpd.conf.port_number` file.
 - b. Open the `httpd.conf.port_number` file in a text editor.
 - c. Modify the port directive to reflect the new port number.
 - d. Save the file and exit.
2. To verify the configuration, perform each of these tests in order.
 - a. In a Web browser, enter `http://hostname:new_port`. You should see the IBM HTTP Web page.

Tip: If the test fails, try pointing the browser to port 80 to verify that the new port went into effect. Look at `httpd.conf`. Make sure that the new Listen statement is there. Restart the IBM HTTP Server.

- b. Enable logging by modifying `cmblogconfig.properties` and verify that all access is taking place through the specified port.

Tip: This properties file is for the IBM Content Manager Toolkit. The Toolkit does not contain the resource manager port number as part of its configuration data, but it might log the port number that it uses for some requests. This information can help you debug a port problem with the eClient or Java API.

- c. Use the eClient or Windows client to retrieve and store a document.

Tip: If the test fails, you must troubleshoot your resource manager. Check the `dklog.log` file for any errors. Make sure that there is a fully qualified hostname in resource manager definition in the system administration client.

Related tasks

“Viewing or modifying an access type” on page 53

Manually synchronizing the encryption key

If you cannot refresh the encryption keys in the system administration client, you might have to refresh them manually.

Symptoms

Refreshing the encryption keys by using the **Refresh Encryption Key** button in the system administration client Library Server Configuration window does not work.

The library server encryption key is no longer synchronized with the resource manager key, so the library server cannot communicate with the resource manager.

Possible causes

There are two possible causes for this problem:

- There might be a configuration problem with the resource manager.

- The resource manager is running but has lost connection with the library server. If this problem happens, the key can be refreshed when the resource manager is restarted.

Actions

Tip: Use the WebSphere Business Integration Server Foundation or WebSphere Application Server **serverStatus** command to see if the resource manager is running. See the information about starting and stopping a resource manager for specific instructions about checking the status of, starting, and stopping a resource manager.

If necessary, complete the following steps to manually update the encryption key:

1. Make sure that the resource manager is running.
2. On the library server, open a DB2 command prompt and enter the following sequence of commands:

```
connect to database
```

where *database* is the name of the library server database

```
select hex(substr(encryptionkey,9,24)) as key from icmstsyscontrol
```
3. Make a note of the 24-character string returned by the select statement and close the connection:

```
terminate
```
4. On the resource manager, open a DB2 command prompt and enter the following sequence of commands:

```
connect to database
```

where *database* is the name of the resource manager database

```
select Hex(substr(acc_public_key,1,24)) as key from rmacess where acc_userid=1
```

```
terminate
```
5. Compare the 24-character string from the library server to the one from the resource manager. If they do not match, enter the following commands, each on its own line, on the resource manager:

```
connect to database
```

where *database* is the name of the library server database

```
update rmacess set acc_public_key=x'string' where acc_userid=1
```

where *string* is the exact string from the library server.

```
terminate
```

DB2 return code -818 during SMS interface utility processing

Errors during SMS interface utility processing might be related to inconsistencies in module time stamps.

Symptom

DB2 return code -818 is received during SMS interface utility processing.

Possible cause

The time stamp in the load module is different from the bind time stamp built from the database request module (DBRM). This problem could happen if the

system staff recently applied maintenance to Multiple Virtual Storage/Data Facility Product and DBRMs were involved.

Action

Complete the following steps:

1. Verify the bind jobs for the new DBRMs.
2. Match the time stamp of new DBRMs against the time stamp of load modules.

Deadlock error SQL0911 RC=2 when importing documents or replicating to a target resource manager

A deadlock error that occurs when importing documents or replicating could be related to the RMTRACKING table.

Symptom

When importing documents or replicating to a target resource manager, error messages like the following messages display in the icrmr resource manager application. The messages show a deadlock during a store request.

```
ICMRM:DEBUG 2004-05-07 10:28:17,403
[Servlet.Engine.Transports:2611] - server id : 3
- java(??)
ICMRM:TRACE 2004-05-07 10:28:17,403
[Servlet.Engine.Transports:2611] -
endtrans processing txid 2004-05-07-14.25.35.343610 - java(??)
ICMRM:DEBUG 2004-05-07 10:28:17,404
[Servlet.Engine.Transports:2611] - endTransTx try 0 - java(??)
ICMRM:ERROR 2004-05-07 10:29:21,808
[Servlet.Engine.Transports:2611] - COM.ibm.db2.jdbc.DB2Exception:
[IBM][CLI Driver][DB2/6000] SQL0911N The current
transaction has been rolled back because of a deadlock
or timeout. Reason code "2". SQLSTATE=40001
- java(??)
COM.ibm.db2.jdbc.DB2Exception: [IBM][CLI Driver][DB2/6000]
SQL0911N The current transaction has been rolled back
because of a deadlock or timeout. Reason code "2".
SQLSTATE=40001
```

Cause

There is a deadlock in the resource manager database in the RMTRACKING table.

Action

You must have the DB2_RR_TO_RS=YES registry variable set in DB2.

1. From a DB2 command prompt, enter the following command: db2set DB2_RR_TO_RS=YES.
2. Restart DB2:
db2stop force
db2start

Error message ICM9712 failed to store documents

If you install the resource manager database and the resource manager application on different machines, you might receive errors when storing documents.

Symptom

After installing the resource manager database and resource manager application on different machines, the following error message displays when attempting to store a document:

```
ICMRM:DEBUG    2006-08-22 23:29:19.465000
context:ICMADMIN:25588317503172253610 [WebContainer :
2] - volume size too small
- getDataAndUpdateVolumeTable(ICMRMDBManager.java:12813)
ICMRM:ERROR    2006-08-22 23:29:19.465000
context:ICMADMIN:25588317503172253610 [WebContainer :
2] - volume space filled -
(RMVolumeNotFoundException.java:40)
com.ibm.mm.icrm.RMVolumeNotFoundException:
volume space filled
```

Cause

The volume is on the resource manager database machine and is not accessible from the resource manager application machine.

Action

Replace the volume with any volume that is accessible from the resource manager application machine.

Enabling the advertisement of byte serving capability for document retrieval to the clients

If you need to serve large PDF documents or if you need to serve documents by using an unreliable Internet connection, then you might need to enable the ability of the resource manager server to advertise byte serving capability to the clients.

Symptoms

The advertisement of byte serving of documents is required only in limited circumstances. However, your content management system might need this capability if you meet both of the following criteria:

- Your organization commonly transfers large documents, up to hundreds of megabytes, by using an Internet connection that is unstable and requires multiple restarts.
- Your organization commonly creates PDF documents with the Adobe Acrobat Fast Web View function enabled for page-at-a-time downloading from web servers.

Causes

Byte serving is a server function that enables clients to request and obtain specific parts of a given document from the server by specifying the starting and ending bytes of those parts. Byte serving is used by some download utility clients to restart requests that are terminated because of unreliable connections. Byte serving is also used by the Adobe Acrobat product family as part of the Fast Web View function.

HTTP protocol allows servers to advertise byte serving capability to clients with an HTTP response header. Beginning with Version 8.2, DB2 Content Manager included a feature that allows the resource manager to perform and advertise byte serving.

Beginning with IBM Content Manager Version 8.4.3, the default resource manager server behavior is changed. The server does not advertise byte serving capability as the default behavior to the clients. The byte serving capability of the server is not affected by this change. The only change is to the advertising of this capability to the clients. However, if you meet the previous criteria, you might need to enable the advertisement of byte serving capability to the clients to revert to the default behavior before Version 8.4.3.

Resolving the problem

Important: Enabling the advertisement of the byte serving capability to the clients can negatively affect the performance of the resource manager in the following ways:

- It can affect the efficiency of the retrieval of PDF documents. A document can be read many times or even many hundreds of times in the case of very large documents before the document is fully retrieved.
- It can cause a significant increase in the number of errors and informational messages in the resource manager logs as the multiple retrieval actions for PDF documents are logged.

To revert to the previous default behavior to advertise the byte serving capability to the clients:

Edit the RMCONFIGURATION system control table and change the setting of the **ADVERTISE_ACCEPT_RANGES** parameter from false to true.

Tip: The option to change this setting for a resource manager is also available as the **Advertise accept ranges** check box on the Definition page of the Resource Manager Configuration Properties window.

Tip: System control tables for the resource manager such as RMCONFIGURATION that begin with the letters "RM" are located in the resource manager database.

Related tasks

"Setting the resource manager definition" on page 56

Troubleshooting resource manager asynchronous jobs

If you experience problems with the running of asynchronous jobs on a z/OS resource manager, you might need to perform troubleshooting tasks to find detailed information about the problem and to determine the corrective action to take.

"Authentication required to run resource manager asynchronous jobs"

"Scheduling asynchronous delete jobs" on page 644

"Troubleshooting collection lists of asynchronous delete jobs" on page 645

Authentication required to run resource manager asynchronous jobs

Before you can run resource manager asynchronous jobs, you must have the right authorization.

Symptom

Users cannot run resource manager asynchronous jobs.

Cause

To run resource manager asynchronous jobs, such as asynchronous delete, asynchronous recovery, and asynchronous replication, you must be authorized.

Action

You must have the AllPrivs privilege set, as well as have the EXECUTE privilege on the library server plans, packages, and procedures, and the resource manager plans. Ensure that you are authorized in the following:

- The JOB card, which is how you get authorized by DB2 Universal Database
- The library server

Related tasks

Customizing resource manager asynchronous processes

Scheduling asynchronous delete jobs

If you schedule resource manager asynchronous delete jobs to run serially and with a specified stop time, you must structure the stop time of the jobs to fit your batch window.

Symptoms

You can schedule asynchronous delete batch jobs to run in series with the same *?STOPTIME?* specification for all jobs. However, the stop time is based on a 24-hour clock. If you do not carefully plan the job stop time, your jobs might interfere with the available batch window.

For example, if a batch job starts at 02:00 AM and has a specified stop time of 08:00 AM, then the first job stops at the specified time, begins to commit, and exits cleanly. The second job starts shortly thereafter, for example, at 08:02 AM. In this case, the job also has a specified stop time of 08:00 AM, but it continues to run until it is complete or until the next 08:00 AM stop time is reached, nearly 24 hours later. These serial jobs might run during peak business hours instead of stopping immediately, which is the preferred outcome of the system programmer.

Causes

All jobs have the same 24-hour clock stop time specified, but the stop time is reached before some of the jobs begin. When a job begins after the specified stop time, it continues to run until it is complete or until the next occurrence of the stop time.

Diagnosing the problem

User response: The system programmer should review the log file for a DEBUG statement that shows Tomorrow: <1> and an INFO statement that shows Stop a day after. This statement means that a job can run for up to 24 hours. If the job is scheduled to end on the same day, the log file shows Tomorrow: <0> and Stop today at.

Resolving the problem

System programmer response: One solution is to change the stop time for each job. Because the jobs are scheduled to run serially, each job should have a stop time argument that is a few minutes after the previous one. For example, the first

job specifies an 08:00 AM stop time, the second job specifies an 08:10 AM stop time, and the third job specifies an 08:20 AM stop time. This method grants enough time for each job to stop cleanly, commit any open work, and terminate before the next job in the queue is scheduled and started.

System administrator response: A second solution involves modifying the JES2 initiator to drain or prevent the asynchronous delete batch jobs from running during peak business hours. For example, to ensure that all of the jobs complete near 08:00 AM, the JES2 initiator that runs this class of jobs must be either drained (\$p) or altered to not handle this class (\$t) every day at 07:59 AM. Re-enable this class of jobs to initiate in the afternoon or whenever the appropriate batch window begins.

Related concepts

The resource manager asynchronous delete process

Troubleshooting collection lists of asynchronous delete jobs

If you specify collection lists of resource manager asynchronous delete jobs, you must verify that the collection names in the list exist and are spelled correctly.

Symptoms

No records were deleted and you see return code=0, reason=0 (no errors) in the asynchronous delete log file.

Causes

The asynchronous delete JCL specifies a collection name that does not exist or is spelled incorrectly. The asynchronous delete log file does not contain an error message when the JCL specifies an invalid collection name, the collection name is misspelled, or the collection does not contain any records.

Resolving the problem

System programmer response: Validate that the collection names exist and are spelled correctly. If the format is correct, the job can run. If one of the collections either does not exist or does not contain any records, the job does not delete any records.

Related concepts

The resource manager asynchronous delete process

Troubleshooting database connection failures on the resource manager

Database connection failures can occur during the startup of the resource manager or during normal resource manager operation. When you experience problems, you might need to perform troubleshooting tasks to find detailed information about the problem and to determine the corrective action to take.

“Troubleshooting database connection failures that occur during resource manager startup” on page 646

“Troubleshooting database connection failures that occur during resource manager operation” on page 646

Troubleshooting database connection failures that occur during resource manager startup

If the database connection fails during the startup of the resource manager, then the data source might not be valid or the database might not be available.

When a database connection failure occurs during the startup of the resource manager, the error is logged in the `SystemOut.log` file. It is also logged in the `icrmr.logfile` file for that resource manager. Use the log data in these files to troubleshoot the failed database connection.

Note: For readability, the log file examples contain line breaks that are not in the actual log files.

The following example shows an excerpt of the errors that are logged in the `SystemOut.log` file for a data source problem:

```
...
0 ICMRM:ERROR There is a problem with RM DB datasource =
java:comp/env/jdbc/RMDatasource, confirm the datasource is valid and
database is started.
0 ICMRM:ERROR java.lang.reflect.InvocationTargetException : Error opening socket
to server xyz123.abc.example.com/127.0.0.1 on port 50000 with message :
null DB2ConnectionCorrelator: nullDSRA0010E:
SQL State = null, Error Code = -4,499 SQLCODE:-4499
...
```

The following example shows an excerpt of the errors that are logged in the `icrmr.logfile` file for a data source problem:

```
...
ICMRM:ERROR 2009-03-30 16:41:39.444000 context: [server.startup : 1] - Problem
with RM DB datasource = java:comp/env/jdbc/RMDatasource, confirm the datasource
is valid and database is started. - initRMContext(ICMResourceManager.java:267)
com.ibm.websphere.ce.cm.StaleConnectionException:
java.lang.reflect.InvocationTargetException :
Error opening socket to server xyz123.abc.example.com/127.0.0.1 on port 50000
with message :
null DB2ConnectionCorrelator: nullDSRA0010E: SQL State = null, Error Code = -4,499
...
```

Related tasks

“Logging and tracing utility: resource manager” on page 400

Troubleshooting database connection failures that occur during resource manager operation

If the database connection fails during the normal operation of the resource manager, then the failure is logged in the `SystemOut.log` file and the WebSphere Application Server First Failure Data Capture (FFDC) log file for the resource manager.

The `SystemOut.log` file contains summary information about the FFDC event that is generated in the FFDC log file.

The FFDC log file contains more detailed information about the problem. The default location for the WebSphere Application Server FFDC log files is in the following path, where `WAS_HOME` is the installation directory of WebSphere Application Server and `profileName` is the name of the profile for the resource manager: `WAS_HOME/profiles/profileName/logs/ffdc`.

Tip: For readability, the log file examples contain line breaks that are not in the actual log files.

The FFDC log file contains information about the resource manager, such as in the following example.

```
com.ibm.ws.rsadapter.spi.WSRdbManagedConnectionImpl.destroy 1005
Exception = com.ibm.db2.jcc.b.DisconnectException
Source = com.ibm.ws.rsadapter.spi.WSRdbManagedConnectionImpl.destroy
probeid = 1005
Stack Dump = com.ibm.db2.jcc.b.DisconnectException: A communication error has been
detected.
Communication protocol being used: T4Agent.sendRequest().
Communication API being used: OutputStream.flush().
Location where the error was detected: Connection reset by peer: socket write error.
Communication function detecting the error:
*. Protocol specific error codes(s) TCP/IP SOCKETS
DB2ConnectionCorrelator: G91E992D.E207.090319145809
...
at com.ibm.mm.icrmr.mdmanager.lsuccess.ALibraryServerConnectionSP.
executeStoreProcedure(ALibraryServerConnectionSP.java:641)
    at com.ibm.mm.icrmr.mdmanager.lsuccess.ALibraryServerConnectionSP.
logon(ALibraryServerConnectionSP.java:177)
```

The FFDC log file also contains information about the database connection, as in the following example:

```
First Failure Data Capture information for
com.ibm.ws.rsadapter.spi.WSRdbManagedConnectionImpl@4020402
```

```
ONE PHASE ENABLED

Database Type:
null

Transaction State:
NO_TRANSACTION_ACTIVE
```

The FFDC log file also contains information about the failing data source in the database, as in the following example:

```
DataSource properties:
{statementCacheSize=10, password=*****, portNumber=50000,
fullyMaterializeLobData=true,
dataSourceClass=com.ibm.db2.jcc.DB2ConnectionPoolDataSource, resultSetHoldability=2,
serverName=cmi275.svl.ibm.com, currentPackageSet=, traceFile=,
dataStoreHelperClass=com.ibm.websphere.rsadapter.DB2UniversalDataStoreHelper,
currentFunctionPath=ICMADMIN, currentSchema=ICMADMIN, driverType=4, description=,
readOnly=false, databaseName=LS8RI275, traceLevel=, user=icmadmin}
```

Related tasks

“Logging and tracing utility: resource manager” on page 400

Troubleshooting replication

Reviewing the known issues related to replication can help you troubleshoot problems if you experience them.

“Items that are checked out are not replicated” on page 648

“Replication return code 7400” on page 648

“ChangeSMS fails on a secondary resource manager” on page 648

“Cannot change or manage replication rules in the public domain” on page 649

“Content Manager Version 8.1 client application receives library server return code 7652” on page 650

“Cannot replicate existing items migrated from Content Manager Version 8.1”
on page 650

“Changing replication rules is not affecting existing items” on page 651

Items that are checked out are not replicated

If an item is checked out, the replicator cannot check it out to replicate it.

Symptom

The replicator is not replicating all items.

Possible cause

The replicator does not replicate items that are checked out. During item replication, the replicator checks out the item. If an item is already checked out, the replicator cannot check out that item, and so cannot replicate it.

Action

The replicator will automatically replicate the item during the next scheduled replication assuming that it can successfully check out the item.

Replication return code 7400

The replication return code 7400 can occur when an item with multiple parts is checked out by a user.

Symptom

You receive return code 7400 from the library server when replicating a document with multiple parts.

Possible causes

Return code 7400 means that the requested item was checked out by another user.

This return code is more likely to occur while replicating documents with multiple parts. For each part, the replicator checks out the item and performs the replication. Therefore, to replicate an item with three parts, the item must be checked out three times to replicate each of the parts.

The replicator can also receive error code 7400 if all of the parts of an item are scheduled to be replicated at the same time. The long-term solution is to schedule replication of different parts sequentially.

Action

No action is required. The replicator will pick up the item in the next replication cycle.

ChangeSMS fails on a secondary resource manager

There are restrictions on the actions that can be performed on a secondary resource manager if the primary resource manager is down.

Symptom

In a replicated environment, ChangeSMS is failing on the secondary resource manager, even though the primary resource manager is down.

Possible cause

When the primary resource manager is down, you can perform only the store, update, and retrieve object operations on the secondary resource manager. You can perform the ChangeSMS operation only on your primary resource manager.

Action

Perform the ChangeSMS operation when the primary resource manager is online and available. If the object for which ChangeSMS is being done was updated, the latest copy must be available on the primary resource manager for the ChangeSMS operation to succeed.

If the target collection is a replica for that object, the primary resource manager moves the object from the source collection to the target collection. This move happens regardless of whether objects exist in the target collection. Also, the item is removed from the replica list in the library server database.

Cannot change or manage replication rules in the public domain

Only superadministrators can change or manage replication rules in the public domain.

Symptom

You cannot change or manage replication rules in the public domain using the system administration console.

Possible causes

Subadministrators can only view the replication rules in public domain. However, you can both view and change the replication rules defined in your own domain, for example, home domain.

The same rules apply to the administration of resource managers and collections. Subadministrators can only view resource managers, collections, and replication rules in the public domain. They cannot change them. However, they can view and change resource managers, collections, and replication rules defined in their own home domain. Superadministrators can view and change resource managers, collections, and replication rules in any of the domains.

Action

Contact a superadministrator to change or manage replication rules in the public domain.

Content Manager Version 8.1 client application receives library server return code 7652

The client application receives library server return code 7652 when it uses a newer server with replication.

Symptom

The Content Manager Version 8.1 client application receives library server return code 7652 when it uses a newer IBM Content Manager server with replication.

Possible causes

The application was compiled and linked with Version 8.1 API libraries and is attempting to create or update an item for a replicated item type, but Version 8.2 API libraries are required.

Replication was introduced in DB2 Content Manager Version 8.2. Therefore, if you have already upgraded your server to Version 8.2 (or later) but not your client, you can continue to create or update items. However, the default resource manager and collection do not have any replication rules associated with it. If replication rules are associated, for example, replication is enabled, Version 8.1 client applications receive library server return code 7652.

Action

Make sure that there are no replication rules associated with the default resource manager and collection in the item type. Upgrading the client application to Version 8.2 or later can also solve the problem.

Cannot replicate existing items migrated from Content Manager Version 8.1

You are unable to replicate items migrated from an older version of Content Manager.

Symptom

You are using Content Manager Version 8.2 or later, and you cannot replicate items that were migrated from Content Manager Version 8.1.

Possible causes

Replication was a new feature for Version 8.2. Therefore, any existing items or documents with parts that were created in Version 8.1 are not automatically enabled for replication.

Action

To enable replication for items that were migrated from Version 8.1, use the resource manager import replicas function to import replication rules for preexisting items.

To use the import replica function, you must manually insert data into a resource manager replication table.

Changing replication rules is not affecting existing items

Replication rules for existing items cannot be changed from the client.

Symptom

A change to the replication rules is not taking effect. Items are being replicated according to the previous replication rules.

Possible causes

When a resource item or object is created, IBM Content Manager applies the current replication rules for that item. When the replication rules are associated with those resource items or objects, there is no way to update the rules using the clients. Any changes to replication rules apply only to new items that are created after the replication rules change.

Action

From a client, you cannot update the replication rules for existing items. One way to work around this restriction is to use the migrator utility for existing items.

For example, assume that the previous rule replicated items from resource manager A collection 1 (resource manager A C1) to resource manager B collection 2 (resource manager B C2). Now you want to replicate from (resource manager A C1) to (resource manager C C3). You can use the migrator to move items from the old target (resource manager B C2) to the new target (resource manager C C3). This action also replaces the old target resource manager (resource manager B C2) in the library server with the new target (resource manager C C3) so that a subsequent replication operation follows the new rule.

Troubleshooting IBM Information Integrator for Content

Problems with IBM Information Integrator for Content can include problems with adding users, retrieving documents, and configuring API logging.

The following topics provide troubleshooting assistance for IBM Information Integrator for Content.

- “Cannot add users to IBM Information Integrator for Content”

- “Cannot retrieve documents larger than 2 MB through IBM Information Integrator for Content V8 to DB2 Content Manager V7.1 server” on page 652

- “Configuring IBM Information Integrator for Content API logging” on page 652

Cannot add users to IBM Information Integrator for Content

Disabling advanced workflow could help you resolve problems with adding users to IBM Information Integrator for Content.

Symptom

You receive error DGL2616A when trying to add users to IBM Information Integrator for Content.

Possible cause

If you remove the IBM Information Integrator for Content database before you delete user IDs and groups from both IBM Information Integrator for Content and MQ Workflow, and then you try to create the same user IDs and groups that existed in the system administration database that you deleted, you get an error stating that the users and groups cannot be added to IBM Information Integrator for Content. The following error message is shown:

DGL2616A: Fail to add the user: XXX -DGL2485A: This workflow user already exists.

Action

Complete the following steps to solve the problem:

1. Disable the IBM Information Integrator for Content advanced workflow service in the system administration client.
2. Log off from the system administration client and log back in. When you log in after disabling the advanced workflow service, you can create the same user IDs and groups that were in IBM Information Integrator for Content and still exist in the MQ Workflow server.
3. Enable the advanced workflow service after you create the user ID and groups that exist in the MQ Workflow server.

Cannot retrieve documents larger than 2 MB through IBM Information Integrator for Content V8 to DB2 Content Manager V7.1 server

If you have problems retrieving documents larger than 2 MB, you might have to increase the value of the FRNHEAPSIZE variable.

Symptom

The following error occurs when attempting to export or retrieve documents greater than 2 MB through IBM Information Integrator for Content Version 8 to the Content Manager Version 7 server: The following message appears:

DGL0368A: Error while retrieving a part, API:SimLibOpenObject
[FRN=8682,ExtRC=0,ReasonCode=0] (STATE) : 0

Possible cause

Insufficient memory is allocated on FRNHEAP.

Action

The IBM Information Integrator for Content DL connector calls the Content Manager C++ Folder Manager API, which uses the FRNHEAP to store memory objects. For large file sizes, more memory is required on the heap. To resolve the problem, you need to increase your FRNHEAPSIZE system variable from the default value of 2048 to a value more appropriate for your environment.

Configuring IBM Information Integrator for Content API logging

If you have problems with IBM Information Integrator for Content API logging, check the logging configuration options available for the APIs and connectors.

“Activating connector logging”

“Working with the logging configuration file” on page 654

“Java log output file example” on page 656

“C++ log output example” on page 658

Activating connector logging

Activating connector logging can help you debug many problems with your content management system applications. To help you isolate problems in a single application, you can override the current log level when you start the application.

The API or connector logging utilities log all exceptions, including those exceptions that are not errors. Occasionally, error messages might appear in the log file that are not propagated to the users. In some cases, the API or user application is able to recover or continue in the case of warnings.

Important: When reading the log files, remember the context within which the exceptions and messages are logged.

Tip: When debugging, you can focus on the current error and events just before that error if you keep the API log file (`dklog.log`) size and content to a minimum. Doing this step can help you to avoid searching a large file and can help increase your speed to resolution.

C++

C++ has one log manager by default. C++ references the same log configuration file as Java does, but the C++ connectors consult only the default log manager logging settings.

On UNIX, when the C++ connector logging utility is first instantiated, it reads the configuration file `cmblogconfig.properties`. This file is located in the `cmgmt/connectors` directory located in the `ibmcmadm` user's home directory. If the configuration file is not found, the default logging settings are used.

On Windows, when the C++ connector logging utility is first instantiated, it reads the configuration file `cmblogconfig.properties` from the `cmgmt\connectors` directory to which `IBMCMROOT` is pointing. If the configuration file is not located, the default logging settings are used.

Java

Java has two log managers: default and `log4j`. You can configure and use only one of the log managers at a time. The same configuration file, `cmblogconfig.properties`, is used to control the type of log manager used and the configuration specific to each type of log manager. For more information about the log manager that you want to use, see the section in the configuration file, `cmblogconfig.properties`, that pertains to the log manager you want to use.

When the connector logging utility is first instantiated, it searches the class path of the Java Virtual Machine instance to find the `ibmcmconfig.properties` file. After this file is found, the API will be able to find the location of `cmblogconfig.properties`, the logging configuration file. If this configuration file is not located, the default logging settings are used.

Overriding the log level with the connect_string parameter

For both C++ and Java applications, you can override the log level value in the cmblogconfig.properties file by entering a new value in the connect_string parameter of the DKDatastoreICM connect() method when you start the application. Overriding the log level by using the connect_string parameter can be useful in debugging situations when you want to debug a single instance of an application. If the application is a C++ application or a Java application that uses the default log manager, you enter DKLogPriority = *log_level* in the connect_string parameter, where *log_level* is the log level. If you are using the log4j log manager in a Java application, you enter DKAPIJavaLogLevel = *log_level* in the connect_string parameter.

Working with the logging configuration file

When you encounter a problem, the API log file, dklog.log, can provide more information to help you investigate the problem.

Setting the trace level in the API log to DEBUG trace setting can greatly increase the speed with which you resolve the problem. The dklog.log file is generated any time IBM Information Integrator for Content is used. Almost every IBM Content Manager application uses IBM Information Integrator for Content APIs, including the system administration client, the Client for Windows, and the eClient.

Requirement: Be sure that you are logged in with, or change to, a user ID that has permission to change the cmblogconfig.properties file.

The cmblogconfig.properties file contains the following default settings:

- It uses the default log manager.
- The default log file name is dklog.log.
- The dklog.log file is placed in the *IBMCMROOT*/log/connectors directory, where *IBMCMROOT* is the installation path for IBM Information Integrator for Content.
- Logging priority is set to Error.
- The maximum number of exceptions of the same error message ID to allow is 5.

You can find the location of the cmblogconfig.properties file by viewing the console information for the application. If the properties file is found on the machine where the application is installed and the ICMFORCECONSOLELOG environment variable is set to true or TRUE, then the path of the properties file is added to the console log after the application starts. If the properties file is not found, then a message stating that the file is not found is added to the console log. A similar message is also added for the icmcmconfig.properties file. The path information for the icmcmconfig.properties file varies depending upon whether the application is a Java or C++ application. For a Java application, the console displays only that the file is found because it does not resolve the part of the path contained in the CLASSPATH environment variable. For a C++ application, the entire path is displayed.

Performance tips

- When the trace setting of the API log is set higher than ERROR, the overall performance is greatly reduced while the system is providing extensive information to the log file. When debugging is complete, reset the API log trace setting to the default level of ERROR or less.

- Delete old IBM Information Integrator for Content logs (dklog.log). When debugging, you can focus on the current error and events just before it if you keep the API log file size and content to a minimum. This step can help you to avoid searching a large file and can increase the speed to resolution.

Modifying the API trace level

To modify the API trace level, you need to edit the `cmblogconfig.properties` file.

Tip: You might need to modify only the log priority settings and retain the default settings for the log file output type, name, and location. This need depends upon your installation configuration.

1. Open the `cmblogconfig.properties` file that is located in *IBMCMROOT* in a text editor.

Tip: Make a backup of the `cmblogconfig.properties` file before you modify it.

2. In section 0 (global settings), specify a maximum exception count. The default value is 5.
3. In section 1 (log manager factory setting), choose between using the default log manager or `log4j`.
4. In section 2.1 (specify log priority), choose a log priority. Priorities range from `DISABLE` to `DEBUG`. The log priority parameter is defined at the end of the section in a key-value pair. If you are using the default logger, the default log priority setting is `DKLogPriority=ERROR`. If you are using the `log4j` logging framework, the default log priority setting is `DKAPIJavaLogLevel=ERROR`. The priorities are:

DISABLE

Disables logging.

FATAL

Provides information that the program encountered unrecoverable errors and must cease operating immediately. Stopping the program is done separately, not from the logging facility.

ERROR

Provides information that the program encountered recoverable or unrecoverable errors, but is able to continue operating.

PERF

Used to collect output information for measuring performance.

INFO

Provides significant event messages, such as successful logon.

TRACE_NATIVE_API

Used for logging before and after a native call. This setting provides parameters and return data information.

TRACE_ENTRY_EXIT

Used for signaling entries and exits of program modules (or code blocks).

TRACE

Used to output additional diagnostic information, such as program state changes, function parameter information, and function return value information.

DEBUG

Used to output information for debugging errors.

5. In section 2.2 (log output destination setting), specify where to log information. The log output destination parameter is defined in a key-value pair. You can choose from three options for DKLogOutputSetting:

- 1 Log to a file.
- 2 Log to Standard Error.
- 3 Log to Standard Console.

The default setting is DKLogOutputSetting=1.

6. If you chose to log to a file (DKLogOutputSetting=1), you must also specify the log file name and log file size settings in section 2.3. Section 2.3 contains two key-value pairs, which define the log file name and output size (in megabytes).

- The default file name is DKLogOutputFileName=dklog.log.
- The default output size is DKLogOutputFileSize=5.

Attention: The log manager continues to append log output into the existing log file. Monitor the size of the file and periodically delete unwanted log output from the log file to prevent the file from becoming too large.

Java log output file example

Use the example to help you understand the information in the log file.

In the log file, error messages are logged in the national language of the user environment. All other diagnostic information is logged in English. The default log file is dklog.log.

Attention: The log text shown here contains line breaks to make it more legible. The actual log file looks slightly different.

The following example shows an INFO section at the beginning of the log file. Each time a program starts, a new INFO entry is added to log file.

Java

```
[EXC]: 08/29/2007 at 21:35:30.642 GMT @ apple (9.xxx.xx.xxx);
com.ibm.mm.sdk.common.DKLogonFailure # com.ibm.mm.sdk.logtool.DKLogManager_Log4J
[USR]: user1 (C:\Documents and Settings\Administrator)
      @ C:\Program Files\IBM\db2cmv8\samples\java\icm
[THD]: main ( 78952e66 )
[THG]: main = { main, Thread-0 }
[LOC]: com.ibm.mm.sdk.server.DKDatastoreICM:logon
[MSG]: DGL0394A: Error in : DKDatastoreICM.connect; [SERVER = icmnlbdb, USERID = icma];
ICM7127: The user ID is not defined or the password is not valid. (STATE) : [LS RC = 7127]
      at com.ibm.mm.sdk.server.DKDatastoreICM.logon(DKDatastoreICM.java:3876)
      at com.ibm.mm.sdk.server.DKDatastoreICM.connect(DKDatastoreICM.java:3430)
      at SConnectDisconnectICM.main(SConnectDisconnectICM.java:240)

[ERR]: 08/29/2007 at 21:35:30.672 GMT @ apple (155.123.9.102);
# com.ibm.mm.sdk.server.DKDatastoreICM
[USR]: user1 (C:\Documents and Settings\Administrator)
      @ C:\Program Files\IBM\db2cmv8\samples\java\icm
[THD]: main ( 78952e66 )
[THG]: main = { main, Thread-0 }
[LOC]: com.ibm.mm.sdk.server.DKDatastoreICM:connect
[MSG]: ?-64:114b38ce6fa:X8000-?-
ERROR: The connect() operation has failed.
      Before exiting the DKDatastoreICM.connect() operation,
      state changes will be rolled back.
Error caught: "DGL0394A: Error in : DKDatastoreICM.connect;
[SERVER = icmnlbdb, USERID = icma];
ICM7127: The user ID is not defined or the password is not valid.
(STATE) : [LS RC = 7127]"

[ERR]: 08/29/2007 at 21:35:30.832 GMT @ apple (155.123.9.102);
# com.ibm.mm.sdk.server.DKDatastoreICM
```

```
[USR]: user1 (C:\Documents and Settings\Administrator)
      @ C:\Program Files\IBM\db2cmv8\samples\java\icm
[THD]: main ( 78952e66 )
[THG]: main = { main, Thread-0 }
[LOC]: com.ibm.mm.sdk.server.DKDatastoreICM:connect
[MSG]: ?-64:114b38ce6fa:X8000-?-com.ibm.mm.sdk.common.DKLogonFailure: DGL0394A:
Error in : DKDatastoreICM.connect; [SERVER = icmnlsdb, USERID = icma];
ICM7127: The user ID is not defined or the password is not valid.
(STATE) : [LS RC = 7127]
      at com.ibm.mm.sdk.server.DKDatastoreICM.logon(DKDatastoreICM.java:3876)
      at com.ibm.mm.sdk.server.DKDatastoreICM.connect(DKDatastoreICM.java:3430)
      at SConnectDisconnectICM.main(SConnectDisconnectICM.java:240)
```

C++

>>>> C++ connector logging started 08/29/2007 at 21:36:47 GMT

```
CODEBASE      : cm83 241_8306      Mon Jul 23 13:58:59 2007
OS version    : Windows version 5.1, build 0 2600, CSDVersion Service Pack 2
CMCOMMON      :
CMBROOT       : C:\Program Files\IBM\db2cmv8
ICMROOT       :
IBMCMROOT     : C:\Program Files\IBM\db2cmv8
PATH          : .;C:\Program Files\IBM\db2cmv8\cmgmt;
C:\Program Files\IBM\db2cmv8\DLL;
C:\Program Files\IBM\db2cmv8\bin;
C:\Program Files\IBM\db2cmv8\java\jre\bin;.
C:\MS.NET2003\Common7\IDE;C:\MS.NET2003\VC7\BIN;
C:\MS.NET2003\Common7\Tools;C:\MS.NET2003\Common7\Tools\bin\prerelease;
C:\MS.NET2003\Common7\Tools\bin;C:\MS.NET2003\SDK\v1.1\bin;
C:\oracle\ora92\jre\1.4.2\bin\client;
C:\oracle\ora92\jre\1.4.2\bin;C:\oracle\ora92\bin;C:\Program Files\Oracle\jre\1.3.1\bin;
C:\Program Files\Oracle\jre\1.1.8\bin;C:\Program Files\IBM\db2cmv8\cmgmt;C:\FRNROOT\TSE;
C:\WebSphereMQ\Java\lib;.C:\PROGRAM FILES\THINKPAD\UTILITIES;C:\WINDOWS\system32;
C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\IBM\Infoprint Select;C:\Utilities
;C:\Notes;C:\Program Files\IBM\Trace Facility\;
C:\Program Files\IBM\Personal Communications\;
C:\Program Files\XLView\;C:\lotus\compent\;C:\WINDOWS\Downloaded Program Files;c:\user
;c:\emacs-20.3.1\bin;c:\rkttools\bin;c:\CMV CDC50\bin;c:\jdk1.4.2\bin;c:\jdk1.4.2\jre\bin;
C:\SQLLIB\BIN;C:\SQLLIB\FUNCTION;C:\SQLLIB\SAMPLES\REPL;C:\user;C:\WebSphereMQ\bin;
C:\WebSphereMQ\WEMPS\bin;C:\FRNROOT;C:\FRNROOT\DLL;C:\FRNROOT\HELP;C:\FRNROOT\BIN;
C:\Program Files\IBM\db2cmv8\inso;C:\Program Files\IBM\db2cmv8;C:\Program Files\IBM\
b2cmv8\bin;C:\Program Files\IBM\db2cmv8\dll;c:\progra~1\beyond~1;
C:\Program Files\IBM\db2cmv8\client;C:\Program Files\Rational\common;
C:\CMV CDC50;C:\Infoprint;
Log Config    : C:\Program Files\IBM\db2cmv8\cmgmt\connectors\cmblogconfig.properties
```

```
[EXC]: 08/29/2007 21:36:48.844 @ apple (155.123.9.102); DKDatastoreAccessError #
[USR]: user1 (C:\Documents and Settings\Administrator)
      @ C:\Program Files\IBM\db2cmv8\samples\cpp\icm
[THD]:      b8c
[PRS]:      42c
[LOC]: (D:\sbroot\src\eip\dk\cmbdbci\db2\PDB2Connection.cpp:ICM::PDB2Connection:
      :throwException):708
[MSG]: DGL0394A: Error in :Error - SQL_ERROR
[IBM][CLI Driver] SQL30082N Attempt to establish connection
      failed with security reason "24"
      ("USERNAME AND/OR PASSWORD INVALID"). SQLSTATE=08001
(STATE) : 08001
```

[08/29/2007 21:36:48.914] b8c E: ?-?-?-

The above error may be expected in some certain scenarios
Trying to connect by using the connect userid from the ini file

```
[EXC]: 08/29/2007 21:36:50.276 @ apple (155.123.9.102); DKLogonFailure #
[USR]: user1 (C:\Documents and Settings\Administrator)
      @ C:\Program Files\IBM\db2cmv8\samples\cpp\icm
[THD]:      b8c
[PRS]:      42c
[LOC]: (D:\sbroot\src\eip\dk\icm\DKDatastoreICM.cpp:DKDatastoreICM::logon):6438
[MSG]: DGL0394A: Error in : DKDatastoreICM.connect [SERVER = icmnlsdb, USERID = icma];
      ICM7127: The user ID is not defined or the password is not valid.
(STATE) : [LS RC = 7127]
```

```
[EXC]: 08/29/2007 21:36:50.276 @ apple (155.123.9.102); DKDatastoreAccessError #
[USR]: user1 (C:\Documents and Settings\Administrator)
```

```

@ C:\Program Files\IBM\db2cmv8\samples\cpp\icm
[THD]:      b8c
[PRS]:      42c
[LOC]: (D:\sbroot\src\eip\dk\icm\DKDatastoreICM.cpp:DKDatastoreICM::logon):6520
[MSG]: DGL0394A: Error in : DKDatastoreICM.connect [SERVER = icm1sdb, USERID = icma];
ICM7127: The user ID is not defined or the password is not valid.
(STATE) : [LS RC = 7127]

[08/29/2007 21:36:50.276]      b8c E: ?-16641150161677764800-?-
DKDatastoreICM::logon(const char* user_name, const char* szPassword,
const char* szNewPassword,const char* datastore_name)
23855384=> !!!WARNING: EXCEPTION PROPAGATED!!!

```

Attention: The log manager continues to append log output into the existing log file. Periodically deleting unwanted log output from the log file can prevent the file from becoming too large.

C++ log output example

Use the example to help you understand the information in the log file.

In the log file, error messages are logged in the national language of the user environment. All other diagnostic information is logged in English. The default log file is `dklog.log`.

Attention: The log text shown here contains line breaks to make it more legible. The actual log file looks slightly different.

The following example shows an INFO section at the beginning of the log file on Windows. Each time a program starts, a new INFO entry is added to log file.

```

[ INFO]
>>>>> C++ connector logging started 05/12/2005 at 18:32:15 GMT

CODEBASE      : vcbase cm83 181MAR11      Fri Mar 11 17:36:36 2005
OS version    : Windows version 5.0, build 0 2195,
               CSDVersion Service Pack 4
CMCOMMON      :
CMBROOT       : C:\IBM\db2cmv8
ICMROOT       :
IBMCMROOT     : C:\IBM\db2cmv8
PATH          : C:\Microsoft\NET2002\Common7\IDE;
               C:\Microsoft\NET2002\VC7\BIN;
               C:\Microsoft\NET2002\Common7\Tools;
               C:\Microsoft\NET2002\Common7\Tools\bin\prerelease;
               C:\Microsoft\NET2002\Common7\Tools\bin;
               C:\Microsoft\NET2002\FrameworkSDK\bin;
               C:\WINNT\Microsoft.NET\Framework\v1.0.3705;.
               C:\IBM\db2cmv8\cmgmt;C:\IBM\db2cmv8\DLL;
               C:\IBM\db2cmv8\bin;C:\IBM\db2cmv8\java\jre\bin;
               C:\FRNROOT\TSE;C:\IBM\db2cmv8\cmgmt;
               C:\Program Files\IBM\WebSphere MQ\Java\lib;
               C:\IBM\JAVA142\bin;C:\PROGRAM FILES\THINKPAD\UTILITIES;
               C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem;
               C:\Program Files\IBM\Infoprint Select;C:\Notes;
               C:\Utilities;C:\Program Files\IBM\Personal Communications\;
               C:\Program Files\IBM\Trace Facility\;C:\SQLLIB\BIN;
               C:\SQLLIB\FUNCTION;C:\SQLLIB\SAMPLES\REPL;
               C:\IBM\CMVDC50;C:\Program Files\IBM\WebSphere MQ\bin;
               C:\Program Files\IBM\WebSphere MQ\WEMPS\bin;C:\ODE50\win;;
               C:\tools;;;C:\IBM\db2cmv8\inso;C:\IBM\db2cmv8;
               C:\IBM\db2cmv8\bin;C:\IBM\db2cmv8\d11;C:\FRNROOT;
               C:\FRNROOT\DLL;C:\FRNROOT\HELP;C:\FRNROOT\BIN;
Log Config    :
               C:\IBM\db2cmv8\cmgmt\connectors\cmblogconfig.properties

```

```
[EXC]: 02/02/2002 at 21:17:15 Pacific
Standard Time @ PINEAPPLE (xxx.x.x.x);
DKDatastoreAccessError 1 # 2
[USR]: ypchen (C:\Documents and Settings\Administrator) 3 @
4 C:\IBMCMROOT\SAMPLES\cpp\ICM\bin
5 [THD]: 1184
6 [PRS]: 948
7 [LOC]: (DKDatastoreICM.cpp):4773
[MSG]: DGL0394A: Error in ::DKDatastoreICM.connect
[SERVER=icmnlsdb:USERID=install] 8 [RC=7127] [ReasonCode=0]
[ExtRC=0] [ExtReasonCode=0] ; (SERVER RC) : 0, (STATE) :
```

This section explains notes 1 through 8 in the C++ error message example.

1. Exception Type (whenever applicable).
2. Log Manager Name (whenever applicable; if the default log manager is used, this field is empty).
3. Login user home directory.
4. Current[®] working directory.
5. ID of thread that reports the error.
6. Process ID.
7. File name: line number.
8. Content server return code.

Attention: The log manager continues to append log output into the existing log file. Periodically deleting unwanted log output from the log file can prevent the file from becoming too large.

Troubleshooting user authentication and access control

Problems with user authentication and access control can include problems with creating and maintaining system users and client users and creating and maintaining access control lists. These problems can also include user logon problems.

The following topics provide troubleshooting assistance for user authentication and access control.

“Cannot define access control lists”

“Client logon attempts causing lockouts” on page 660

“System accounts and passwords” on page 661

“Error occurred while updating user” on page 664

“Error: supplied credentials invalid” on page 664

“Error SQL0964C when trying to enable public access” on page 665

Cannot define access control lists

To define access control lists, you must have the correct privileges.

Symptom

You cannot define access control lists (ACLs).

Possible causes

You do not have the correct privileges to define ACLs. The privilege requirement depends on whether administrative domains are enabled or not:

- When administrative domains are disabled, only superadministrators can create access control lists and privilege sets.
- When administrative domains are enabled, you must belong to the SuperDomain. The SuperDomain is where you can manage system objects for all domains and define access control lists or privilege sets. If you do not belong to the SuperDomain, you must have the specific privilege to create access control lists or privilege sets for a domain. Subadministrators cannot perform these actions.

Action

Ask an administrator with the appropriate privileges to define the ACLs.

Related concepts

“Administration authority” on page 429

Client logon attempts causing lockouts

Client lockout problems can be related to the value of the ICMSEVERREPTYPE parameter and the lockout settings on the library server operating system.

Symptoms

Users are confused about which password to use to connect to IBM Content Manager.

User accounts on the system with the library server are being locked out, but the users can still connect to IBM Content Manager.

Possible cause

Depending on how your system is configured, your users might be confused about what user ID and password to use. This situation might result in lockout problems when connecting from any client, including custom clients. Factors include:

- Value of the ICMSEVERREPTYPE parameter in cmbicmsrvs.ini
- Lockout settings on the library server operating system

Authentication is made in two steps, which are not noticeable to your users. First, a connection is made to DB2. Then the user ID and password are passed to Content Manager EE.

The connection to DB2 is made with either the user ID and password provided for the logon or with the shared database connection ID, ICMCONCT. The ICMSEVERREPTYPE parameter in cmbicmsrvs.ini controls how connections are made to the library server. The options for this parameter include the following values: DB2, DB2CON, ORACLE, and ORACON.

Because Oracle user IDs are not operating system IDs, this situation does not develop with an Oracle library server.

DB2

When DB2 is specified, the connection is first attempted with the password that the user provides on the logon screen. The password provided in this instance must be valid for connection to DB2. If it is not valid, the connection is made instead with the shared database connection ID.

After the connection to DB2 has been established, the password is checked by IBM Content Manager. If it is valid within IBM Content Manager, the user logs on successfully. If it is not valid, logon fails and an error message displays.

Although the user never noticed it, an attempt was made to log on to the operating system and it failed. On systems that are set up to lock out users after a certain number of consecutive failed logon attempts, this failure counts as a failed logon attempt.

DB2CON

When DB2CON is specified, the connection is made initially with the shared database connection ID. Then the user ID and password that were provided on the logon screen are passed to IBM Content Manager for authentication. This method removes the possibility of a lockout from the operating system, because the shared connection ID should always connect successfully.

If the IBM Content Manager password is not valid, the user receives an error message indicating that the logon failed.

Actions

The following options are available to you to stop inadvertent lockouts. Choose the one that best suits your requirements.

- Set up IBM Content Manager user IDs to use the operating system password and instruct your users to log on with their operating system passwords. Users will not be confused by having multiple accounts.
- Set ICMSEVERREPTYPE to DB2CON and instruct your users to log on with their IBM Content Manager passwords. The connection to DB2 will always be made with the shared connection ID and there will be no lockouts on the operating system. If a user does try to log on with the wrong password, it is only evident in IBM Content Manager.
- Use client authentication for DB2. Because the authentication takes place on the client system, the user cannot be locked out of the library server.

Attention: There are security implications that you must consider about using client authentication for DB2. See the DB2 Universal Database Information Center for a discussion of authentication in DB2.

Tip: User accounts within the IBM Content Manager system can also be configured to lock after a certain number of failed logon attempts. To set up account lockout on the library server, change the **Maximum logon attempts** value in the library server configuration. To unlock an IBM Content Manager account, log in to the system administration client and reset the password associated with the user ID.

Related tasks

“Viewing or modifying the configuration parameters” on page 6

“Resetting user passwords” on page 461

Related information

 Authentication in DB2

System accounts and passwords

Review the system accounts and passwords information to learn about the configuration and function of the different system accounts.

IBM Content Manager and IBM Information Integrator for Content use several different accounts and passwords to access different components. These accounts and passwords are normally created during installation. Change the passwords in accordance with the security guidelines of your organization.

Recommendation: Periodically, you should change passwords for security purposes. In addition to following the security guidelines of your organization, consider changing passwords under the following circumstances:

- After installation
- After an upgrade
- When a password has been compromised

Shared connection ID account (ICMCONCT)

The shared connection ID is used by users who do not have individual DB2 user IDs. This account is an operating system user who should have minimal permissions. The password is saved as an encrypted string in the shared connection ID file.

Table 87. Shared connection ID files

Product	File name	Location
IBM Content Manager	cmbicmenv.ini	IBMCMROOT
IBM Information Integrator for Content	cmbfedenv.ini	IBMCMROOT

To change the IBM Content Manager or IBM Information Integrator for Content shared connection ID password, you can use the system administration client.

In the system administration client, click **Tools > Manage Database Connection ID > Change Shared Database Connection ID** to open the Change Shared Database Connection ID and Password window.

The default account name is ICMCONCT, but you can change that. If you rename the ICMCONCT user, substitute the new name for icmconct in the command to update the password.

Library server and administration database administrator accounts

A system can have multiple administrators, each with their own user IDs and passwords. The method for changing the password of an administrator depends on what type of administrator the account is and how the account was defined.

There are two types of administrators, superadministrators and subadministrators. Superadministrator accounts are always defined in the operating system. Subadministrator accounts can be defined in the operating system (with minimal permissions) or within the IBM Content Manager or IBM Information Integrator for Content system. When defined in the operating system, these accounts should have only minimal permissions.

Resource manager database account

The resource manager accesses the database with this account, which is an operating system account on the system with the database. This account should have minimal permissions. The password is stored as an encrypted string in a file

on the resource manager. To change the password, update the data source definition using the WebSphere Application Server administration console.

Resource manager administrator password

This password does not belong to an operating system account. The password is stored in the resource manager database and is stored as a property of the resource manager on the library server. It is stored as an encrypted string in both places. To change the resource manager administrator password, complete the following steps:

Important: You must change the passwords in the indicated order or the library server is be unable to communicate with the resource manager.

1. In the system administration client, click **Server Definitions**. Right-click the resource manager server in the right pane and select **Properties**. Change the password in the **Password** field in the Server Definition Properties window. This step changes the password stored on the resource manager.
2. Right-click your resource manager in the left pane and select **Properties**. Change the password in the **Password** field in the Resource Manager Properties window. This step saves the password in the library server.

Media archive password

This password, which does not belong to an operating system account, is stored as an encrypted string in the resource manager database. To change it:

1. Change the password on the media archive server.
2. Update the server definition properties for the media archive server in the system administration client.

Text search password

If you change the password for DB2 Version 7 Text Information Extender or DB2 Version 8 Net Search Extender, you must update the password in the system administration client. Update the password stored in the library server configuration information.

Tivoli Storage Manager password

This password, which does not belong to an operating system account, is stored as an encrypted string in the resource manager database. To change it:

1. Change the password in Tivoli Storage Manager.
2. Update the server definition properties for the Tivoli Storage Manager server in the system administration client.

DB2 Content Manager VideoCharger password

This password, which does not belong to an operating system account, is stored as an encrypted string in the resource manager database. To change it:

1. Change the password in DB2 Content Manager VideoCharger.
2. Update the server definition properties for the DB2 Content Manager VideoCharger server in the system administration client.

Related concepts

“Starting and stopping a resource manager” on page 371

Related tasks

“Changing the library server and system administrator password to the resource manager” on page 16

“Viewing or modifying the library server configuration” on page 6

“Viewing or modifying resource manager properties” on page 52

“Viewing or modifying a server definition” on page 63

“Changing your password” on page 119

“Viewing or modifying a media archive volume” on page 341

“Viewing or modifying a Tivoli Storage Manager volume” on page 345

“Viewing or modifying a DB2 Content Manager VideoCharger volume” on page 339

“Changing the shared database connection ID and password” on page 431

Error occurred while updating user

Changes to a user definition must be done by a different user.

Symptom

When users try to edit their own user definitions, they receive a DGL3804 error.

Possible cause

Users cannot change their own user definitions.

Actions

A user can change a user definition for another user only if the user who wants to change the user definition has a privilege set that contains the following privileges:

- SystemDefineUser
- SystemDomainQuery
- SystemQueryUserPrivs

An administrator can change a user definition for another user.

Error: supplied credentials invalid

The supplied credentials error is usually related to a problem with LDAP configuration.

Symptom

When you install IBM Content Manager Version 8, you get the following message:
The Supplied Credentials are not valid.

When connecting to JDBC to verify existence of the library server database, you get the following error:

The Supplied Credentials are not valid.

Action

This problem usually occurs when your system is set up to use an LDAP server. Even though you might not want your IBM Content Manager system to use LDAP, it looks at your DB2 Universal Database configuration to see if you are using LDAP. Therefore, you might receive the following error message:

```
Connecting to JDBC to check LS/DB existence.  
The Supplied Credentials are not valid. Common causes  
include an offline LDAP server.
```

Check your DB2 Universal Database environment variables by entering the following command at a DB2 command prompt:

```
db2set -all
```

If the environment variable DB2_ENABLE_LDAP is set to **YES**, set it to **NO** by entering the following command at a DB2 command prompt:

```
db2set DB2_ENABLE_LDAP=NO
```

You can now install IBM Content Manager. You should configure LDAP after you have successfully installed IBM Content Manager.

Error SQL0964C when trying to enable public access

An error that occurs when you try to enable public access might be related to the number of item types or views in the library server database.

Symptom

Attempting to change the public access enabled library server configuration value in a DB2 library server database generates the following error:

```
SQL ERROR: SQL0964C The transaction log for the database  
is full. SQLSTATE=57011 <SQL0964C The transaction log for  
the database is full. SQLSTATE=57011> <SQLSTATE 57011:  
Virtual storage or database resource is not available.>
```

Possible cause

This error can occur when there is a large number (greater than 1300) of item types or views in the library server database. The problem is caused by the regeneration of view access information for all component views when the public access enabled control parameter is changed.

Action

The recommended solution is to increase the number of secondary log files.

1. Open a DB2 command prompt.
2. At the DB2 command prompt, enter the following command to obtain the DB2 log file configuration:

```
get db cfg for db_name
```

Substitute the name of the library server database for the *db_name* variable.
3. DB2 returns information about the database. Review the log file configuration. For example, the following results show the default settings for a library server database. This database uses 30 log files (10 primary and 20 secondary). Each log file is 4 MB in size (1000 times 4 KB).

Log file size (4KB)	(LOGFILSIZ) = 1000
Number of primary log files	(LOGPRIMARY) = 10
Number of secondary log files	(LOGSECOND) = 20

4. Enter the following command at the DB2 command prompt to increase the LOGSECOND value:

```
update db cfg for db_name USING LOGSECOND new_value
```

Guideline for selecting *new_value*: 100 secondary log files are typically sufficient for a database with 1300 item types and 6000 component views.

5. Restart DB2 using the db2stop and db2start commands and try the operation again. Changing the public access setting can still take a long time if there are many views. For example, it might take an hour to regenerate the views in a database with 6000 components.

Troubleshooting LDAP integration

Problems with LDAP integration can include problems with the import scheduler and with user authentication.

The following topics provide troubleshooting information about LDAP integration.

“Finding the log files that help with LDAP troubleshooting”

“Troubleshooting authentication problems with the LDAP user preauthentication tool” on page 667

“Running the LDAP user import utility with the correct user privileges” on page 668

“LDAP user import scheduler save function fails” on page 669

“Problems with the LDAP import utility schedule on non-English Windows operating systems” on page 669

“Scheduled LDAP import does not launch on Windows” on page 670

“Using log files for problem diagnosis if LDAP user authentication fails” on page 670

“Resource manager LDAP authentication is failing” on page 672

“Users cannot connect after you import users from LDAP” on page 673

“Authentication of users fails when using the common name user attribute with Active Directory” on page 674

“Incorrect password entries cause account lockouts earlier than expected” on page 675

Finding the log files that help with LDAP troubleshooting

The integration of Content Manager EE with LDAP involves several different components of Content Manager EE. Therefore, if you discover problems during LDAP integration or after your system is running with LDAP, there are several different log files that you might need to review to diagnose the problems.

LDAP configuration and LDAP import in the system administration client

Problems related to the LDAP configuration that generates the information for the cmcmenv.properties file and problems related to the manual import of LDAP users are logged in the following file:

IBMCMROOT/log/sa/cmadmin.log

A related file that you might also want to check when diagnosing problems is the following file:

IBMCMROOT/cmgmt/cmbcmenv.properties

LDAP user import scheduler

Problems related to the automatic LDAP user import scheduler are logged in the following files, where *DB_name* is the library server database name and *server_type* is the server type, with a value of ICM for Content Manager EE and Fed for IBM Information Integrator for Content:

IBMCMROOT/log/sa/ldapimportutil.log

IBMCMROOT/admin/common/cmldapimptool81.stderr

IBMCMROOT/admin/common/cmldapimptool81.stdout

IBMCMROOT/admin/common/cmldapimpusers81.DB_name.server_type.stderr

IBMCMROOT/admin/common/cmldapimpusers81.DB_name.server_type.stdout

A related file that might also contain log entries for problems with the LDAP user import scheduler is the following file:

IBMCMROOT/log/connectors/dklog.log

LDAP user authentication

Problems related to LDAP user authentication are logged in the following files:

Windows based library server: c:\UE.LOG

UNIX based library server: /tmp/UE.LOG

IBMCMROOT/log/ls/icmserver.log

Important: To generate and use the UE.LOG file for LDAP user authentication problem diagnosis, the LDAP log facility must be enabled.

Related reference

“Using log files for problem diagnosis if LDAP user authentication fails” on page 670

Troubleshooting authentication problems with the LDAP user preauthentication tool

The LDAP user preauthentication tool can help you confirm that the LDAP authentication for Content Manager EE is configured correctly.

The LDAP user preauthentication tool is an interactive tool that helps you check different aspects of the configuration for LDAP authentication. The tool contains three tasks:

- Task 1 helps you check that the *cmbcmenv.properties* property file is moved to a remote library server machine as required. The properties file is required for user authentication. When you run this task, the tool checks whether the property file is in the correct location and helps you move the file to the correct location if it is not found.
- Task 2 helps you check that the IBM Tivoli Directory Server client is installed correctly on the library server machine. The IBM Tivoli Directory Server client is required for LDAP authentication within Content Manager EE, regardless of the

type of LDAP server that your system is using. When you run this task, the tool checks whether the required client is installed and provides guidance for installing the client if it is missing.

- Task 3 helps you check that your LDAP integration is complete by authenticating an LDAP user to the Content Manager EE system. When you run this task, the tool asks for an LDAP user name and password, attempts to log on, and shows the result of the attempt.

The LDAP preauthentication tool is packaged with the system administration component and runs on the machine where the system administration client is installed. It is available in the *IBMCMROOT\bin* path. You run the LDAP preauthentication tool as a batch or shell script, depending upon the operating system on the system administration client machine. The tool runs in the console as a command line tool.

Important: If the library server is on a remote machine, not on the same machine with the system administration client, the LDAP user preauthentication tool requires an FTP server to be installed on the library server machine. The FTP server must be running on port 21.

To run the LDAP preauthentication tool, enter the following command, using the .bat or .sh extension as appropriate for your operating system. The following example command is for a system administration client machine with a Windows operating system:

```
cmldaptool.bat
```

The LDAP preauthentication tool provides a menu of options for the tasks and other usage information when it starts.

Related reference

“Finding IBMCMROOT” on page 571

Running the LDAP user import utility with the correct user privileges

The user that runs the LDAP user import utility must have the proper privileges.

Symptom

Is there a way to avoid granting domain admin privileges to the user that is running the LDAP user import utility?

Action

The user that runs the user import utility is an LDAP root user, not an IBM Content Manager user. The user must be an LDAP root user, or a user with domain admin privileges. This requirement exists because the utility needs to perform synchronization and authentication across active directory (LDAP server), and LDAP requires that the user have this full authorization.

A normal LDAP user, or the domain user, does not have the proper authority and is not allowed to perform the LDAP synchronization and authentication processes. This behavior is a limitation of the LDAP server, rather than IBM Content Manager.

LDAP user import scheduler save function fails

If the creation of the CRON job for the LDAP user import scheduler fails, you can create the CRON job manually.

Symptom

When running the LDAP (Lightweight Directory Access Protocol) user import scheduler on UNIX, the LDAP creates a CRON job for the logged-on user, but fails because the *IBMCMROOT/admin/common/csaldapimptool.task* file cannot be written.

Action

When this problem happens, you can manually create a CRON job by completing the following steps:

1. Enter `crontab -e` to open a new file.
2. Enter the following command:

```
10 10 * * 1,2,3,4,5,6,0 /usr/CM83/admin/common/cmldapimpusers81.sh
database ICM
```

where *database* is your library server database name.

Problems with the LDAP import utility schedule on non-English Windows operating systems

The LDAP import utility might have problems if the parameters for the Windows AT command are translated.

Symptom

When creating an import schedule for the LDAP import utility on Windows, users on non-English operating systems might have problems.

Possible cause

On Windows, the schedule is created using the **AT** command. The **AT** command uses the following parameters:

- For weekly use, the command uses M, T, W, Th, F, S, Su
- For daily use, the command uses 1 - 31

Some languages might translate the parameters, causing problems with the tool usage.

Action

To fix this problem, you can use the schedule task function in the user interface to review and verify that the schedule was set correctly.

1. Click **Start > Control Panel > Scheduled Tasks**.
2. Click the name of the LDAP import schedule file.
3. Click **Schedule** and select the days and time you want the task to run, or verify that the information displayed is correct.

Scheduled LDAP import does not launch on Windows

If the LDAP import utility does not run as scheduled on Windows, there might be a problem with the setup of the AT service account.

Symptom

You are using the LDAP import utility to schedule a time to import users, but sometimes the scheduled task is not launched at the scheduled time.

Possible causes

The task is actually saved in the scheduled tasks of the operating system. The reason is that the AT service account, which is the scheduled task account, did not use the account for the logged on user. The AT service account was therefore set to system account.

Action

You need to set the AT service account to your account. Use the following steps to set the AT service account on Windows:

1. Click **Start > Settings > Control Panel**.
2. Double-click **Scheduled Tasks**.
3. From the menu bar, click **Advanced > AT Service Account**.
4. Click **This Account**.
5. Enter your password in the **Password** and **Confirm Password** fields.

The user account that you specify must have the appropriate privileges to run any tasks that you schedule using the **AT** command. For example, if you schedule programs that only administrators can run, you must specify an administrator account.

Using log files for problem diagnosis if LDAP user authentication fails

When users cannot log on with LDAP user authentication, there might be errors in the configuration parameters. You can find information about the problem and how to solve it by using the log files.

Symptom

The LDAP user authentication process fails, and users cannot log on to a server.

Possible cause

Errors in the LDAP configuration parameters might exist.

Actions

1. Check that the LDAP exit routine is executing.
 - a. Turn on tracing for the library server and try again to log on.
 - b. View the log file. Verify that the file ICMXLSLG.DLL exists in the directory indicated in the DLL Path entry in the log file. If it does not exist in this location, see the LDAP integration steps, including the step to install the user exit for LDAP authentication.

c. In the log file, look for the ICMPLSLG CallUserExit entry.

If the entry is not present, the LDAP exit routine was not called. There is a problem with the LDAP configuration. See the LDAP integration steps, including the steps to generate and install the properties file and the step to install the user exit for LDAP authentication.

If the entry is present, then the LDAP exit routine was called but it was not successful. Continue with the next step.

2. Enable the LDAP log facility on the library server.

If you experience failures with LDAP user authentication, you can further analyze why LDAP user authentication is failing by setting the LDAP log to debug for better troubleshooting analysis. Setting the LDAP log to debug creates the UE.LOG log file on the machine where the library server is installed. On a Windows system, the UE.LOG file is written to C:\UE.LOG. On a UNIX system, the UE.LOG file is written to /tmp/UE.LOG.

The UE.LOG file traces each step of the LDAP user authentication process. When authentication is failing, the UE.LOG file provides information that can guide you with debugging the problem. The log file also captures detailed information about other LDAP processes, such as importing users.

You can set the LDAP log to debug by using two different procedures, by setting an integer value for the library server logging level in the log configuration utility or by setting the value of the LDAPDEBUG environment variable. The recommended procedure is to set a value on the logging level because it does not require a restart of the library server or database.

After LDAP authentication is operating successfully and users are able to log in with no error messages, disable the LDAP log facility. Generating the UE.LOG file each time that a user is authenticated slows system performance. Choose one of the following options, based upon how the LDAP logging was enabled:

- To disable LDAP logging from the library server logging level in the log configuration utility, use the steps for changing the logging level to change the integer value to one of the predefined logging levels for the library server, such as **Error** or **Warning**.
- To disable LDAP logging from the LDAPDEBUG environment variable, use the steps for Windows or UNIX systems to set the value of LDAPDEBUG equal to 0. Alternatively, you can remove the environment variable from the system.

Enabling LDAP logging dynamically from the library server logging level

To enable LDAP logging by setting the logging level for the library server in the log configuration utility:

1. From the system administration client, click **Tools > Log Configuration**.
2. Click **Library server**.
3. In the **Logging level** field, enter the following value and save the settings: 4096.

Enabling LDAP logging on Windows systems

To enable LDAP logging by setting the LDAPDEBUG system variable for a Windows environment:

1. Log on to the Windows machine where the library server is installed with a user ID that has administrator privileges.
2. Click **Start > Settings > Control Panel** and open **System**.

3. Create a system variable. Enter LDAPDEBUG in the **Variable** field and 1 in the **Variable Value** field.
4. Save the variable.
5. Restart the system.

Enabling LDAP logging on UNIX systems

To enable LDAP logging by setting the LDAPDEBUG system variable for a UNIX environment:

1. Log on to the UNIX system where the library server is installed with a user ID that has DB2 administrator privileges, or log on as the root user.
2. Change to the `/home/DB2INSTANCE/sqllib/` path where *DB2INSTANCE* is the DB2 instance name.
3. Make a backup copy of the `userprofile` file.
4. Open the `userprofile` file in a text editor.
5. Modify the `userprofile` file by adding the LDAPDEBUG variable name and value information. For example, add `export LDAPDEBUG=1`.
6. Add LDAPDEBUG to the DB2ENVLIST in `/home/DB2INSTANCE/sqllib/profile.env` path.
7. Verify that the export variables for ICMDLL and IBMCMROOT contain the correct path values for your UNIX system.
8. Restart DB2 Universal Database to ensure that the new LDAPDEBUG environment variable is picked up in the environment.

Related tasks

“Integrating LDAP with Content Manager EE” on page 436

Resource manager LDAP authentication is failing

A failure of LDAP authentication on the resource manager might be because of expired LDAP access passwords.

Symptom

When you try to connect to a resource manager through the system administration client, you see the following message:

Get output stream for connection to resource manager failed.

Possible cause

LDAP authentication might have failed with the resource manager.

Action

Update the access passwords by modifying the LDAP `cmbcmenv.properties` file.

Attention: IBM Content Manager installs two files named `cmbcmenv.properties`. One `cmbcmenv.properties` file contains configuration path information and is installed in the *IBMCMROOT* directory. You *do not* modify this file. The other `cmbcmenv.properties` file contains the LDAP configuration parameters and is installed in a path that begins with the WebSphere Application Server home directory. You *do* modify that file.

To update the access passwords, perform the following steps:

1. Notify system users that you plan to stop the resource manager and WebSphere Application Server. Users cannot send requests to or receive documents from the resource manager while you update the access passwords.
2. Stop the resource manager and WebSphere Application Server through the WebSphere Application Server administration client.
3. Navigate to the `cmbcmenv.properties` file in your WebSphere Application Server home directory. You must have write access to all levels of the WebSphere Application Server home directory where the `cmbcmenv.properties` file is located.

The installation location varies by operating system, but the file is always located in the `/installedApps/node_name/icmm.ear/icmm.war/WEB-INF/classes/com/ibm/mm/` path in the installation location.

Operating system	Default WebSphere Application Server installation location
AIX	<code>/usr/WebSphere/AppServer</code>
Linux	<code>/opt/WebSphere/AppServer/profiles/RM_PROFILE</code>
Solaris	<code>/opt/WebSphere/AppServer</code>
Windows	<code>c:\Program Files\IBM\WebSphere\AppServer</code>

4. Back up `cmbcmenv.properties` before you change any information.
5. Update the `LDAP_SECURITY_CREDENTIALS` parameter for the user ID that is trying to connect and failing. Delete the encrypted password and update it to be non-encrypted. (When you restart WebSphere Application Server, it automatically encrypts the password again.)
6. Save the updated file.
7. On the server where the resource manager is installed, log on with a user ID that has DB2 administrative (DBADM) authority. If required, catalog the resource manager database to your local system.
8. Connect to the resource manager through a DB2 command prompt:


```
connect to rmdbname user user_ID using password
```

 where *password* is the original password assigned when the resource manager was created. Do not try to connect using the password that you changed in `cmbcmenv.properties`.
9. Search for the user ID values stored in `RMAccess`. Update the existing password associated with the user ID of the person who experienced the resource manager connection failure. The `RMAccess` table can contain multiple user IDs. Before you can update the password, you must know the `ACC_USERID` value. To find the `ACC_USERID` value, enter the following command at a DB2 command prompt:


```
select * from RMAccess
```

 DB2 returns a record listing all the user IDs. The `ACC_USERID` value is the number to the left of the user IDs listed in the records returned from the `RMAccess` table.

Users cannot connect after you import users from LDAP

If LDAP users cannot use IBM Content Manager workflow, there might be configuration errors in the required products.

Symptom

After you import users from LDAP, users cannot connect to use IBM Content Manager workflow under WebSphere Portal content publishing.

Possible cause

Errors during configuration of products required for IBM Content Manager workflow in WebSphere Portal content publishing can cause this problem.

Action

Try the steps in this section to verify correct configuration. The steps assume that you use IBM Directory Server Version 4.1 and IBM Content Manager Version 8.1 or later.

1. Start the system administration client and verify two settings:
 - Check the library server configuration by clicking **Library Service Parameters > Configurations**. Ensure that **Allow trusted logon** is selected.
 - Verify the properties for your database connection user ID. The default user ID is ICMCONCT. Click **Authentication > Users**. Make sure that the user has the UserDBTrustedConnect privilege set.
2. Verify that you can connect to the database from a command prompt by using the database connection user ID user and password. If you do not know which user ID or password was specified when IBM Content Manager was installed, you can change the user ID or password by clicking **Tools > Change Database ID/password** in the system administration client.
3. Verify that your LDAP server is started.
4. In a Web browser, enter `http://fully_qualified_hostname/webapp/examples/showCfg`. If the showCfg page displays, security is correctly configured.

Authentication of users fails when using the common name user attribute with Active Directory

Microsoft Active Directory user authentication might fail because of the way that the common name attribute is sometimes used within Active Directory.

Symptom

Microsoft Active Directory authentication of users fails.

Possible cause

The default user attribute for IBM Content Manager LDAP configuration is *cn* (common name). However, within Active Directory the *cn* attribute entry can be different from the actual user ID, depending on the LDAP server configuration. This difference can cause the user authentication to fail.

Action

Change the user attribute to *samaccountname* so that Active Directory verifies against the user ID instead of the common name.

To change the default value to *samaccountname*:

1. Log on to the system administration client.

2. Go to **Tools > LDAP Configuration > Server**
3. Change the user attribute from *cn* to *samaccountname*.
4. Save the changes.
5. Import the LDAP user and log on to the Client for Windows.

After you make the change to use the *samaccountname* attribute, ensure that the LDAP integration is correct by repeating all steps for LDAP integration.

Related tasks

“Integrating LDAP with Content Manager EE” on page 436

Incorrect password entries cause account lockouts earlier than expected

When a user enters an incorrect password during authentication with the LDAP server, the number of authentication attempts allowed by the server is fewer than what is expected by the user. The result might be that a user is locked out of a user account earlier than they expect to be with an incorrect password entry.

Symptom

The ICMXSLG.DLL user exit sends user information to the LDAP server for authentication. The default behavior of this user exit is to attempt to send the password to the LDAP server two times if the password is entered incorrectly. For some content management systems that are integrated with LDAP, the LDAP server has a strict password policy, and the second attempt by the user exit to authenticate the password can cause users to be locked out of their accounts earlier than they expect.

Actions

If you need to change the behavior of the ICMXSLG.DLL user exit, you can use the NOINDIRECT system variable. To enable the second authentication attempt by the ICMXSLG.DLL user exit, set the value to 0. To disable the second authentication attempt by the ICMXSLG.DLL user exit, set the value to 1.

Disabling the second authentication attempt on Windows systems

To disable the second authentication attempt by setting the NOINDIRECT system variable for a Windows environment:

1. Log on to the Windows machine where the library server is installed with a user ID that has administrator privileges.
2. Click **Start > Settings > Control Panel** and open **System**.
3. Create a system variable. Enter NOINDIRECT in the **Variable** field and 1 in the **Variable Value** field.
4. Save the variable.
5. Restart the system.

Disabling the second authentication attempt on UNIX systems

To disable the second authentication attempt by setting the NOINDIRECT system variable for a UNIX environment:

1. Log on to the UNIX system where the library server is installed with a user ID that has DB2 administrator privileges, or log on as the root user.
2. Change to the `/home/DB2INSTANCE/sqllib/` path where `DB2INSTANCE` is the DB2 instance name.
3. Make a backup copy of the `userprofile` file.
4. Open the `userprofile` file in a text editor.
5. Modify the `userprofile` file by adding the `NOINDIRECT` variable name and value information. For example, add `export NOINDIRECT=1` to disable the second authentication attempt.
6. Add `NOINDIRECT` to the `DB2ENVLIST` in `/home/DB2INSTANCE/sqllib/profile.env` path.
7. Verify that the export variables for `ICMDLL` and `IBMCMROOT` contain the correct path values for your UNIX system.
8. Restart DB2 Universal Database to ensure that the new `NOINDIRECT` environment variable is picked up in the environment.

Troubleshooting document routing processes

Problems with document routing processes can include problems with synchronization and problems with workflow creation and modification.

The following topics provide troubleshooting information about document routing processes.

- “Cannot start MQ Workflow server with `cmbwfstart` command”
- “Failed to synchronize users with `EIPUser2WF.bat`” on page 677
- “Failure to create workflow or retrieve workflow template” on page 678
- “Icon is reset each time the icon is dropped on the drawing surface in the workflow builder” on page 679
- “Workflow builder does not have work node variables listed in the Decision Point window” on page 679
- “Incorrect routing of first document in a workflow” on page 679
- “Document routing performance problems during updates” on page 680

Cannot start MQ Workflow server with `cmbwfstart` command

If you are not using the default name for the system administration database, then the `cmbwfstart` command might not work.

Symptom

Cannot start the MQ Workflow server with the `cmbwfstart` command.

Possible cause

The `cmbwfstart` command does not work properly if the name of your system administration database is not `icmnsdb` (the default name).

Action

1. Locate the `cmbwfstart` command file for your operating system. If you do not already have a copy on your system, the files are located on the IBM Information Integrator for Content CD, in the `WFIInstall` directory.

2. Modify the **cmbwfstart** command file to add the **-d databasename** option, where *databasename* is the name of your IBM Information Integrator for Content system administration database.

Operating system	Command	Modify this line
AIX	CMBWFAIXSTART.sh	<i>IBMCMROOT/workflow/cmbupes81.sh -d databasename</i>
Solaris	CMBWFSUNSTART.sh	<i>IBMCMROOT/workflow/cmbupes81.sh -d databasename</i>
Windows	cmbwfstart.bat	@call "%IBMCMROOT%" \cmbupes81.bat -u %CMBUPESUSER% -p %CMBUPESPASS% -d <i>databasename</i>

Failed to synchronize users with EIPUser2WF.bat

Errors with the synchronization of IBM Information Integrator for Content users with the MQ Workflow server might be related to the number of users.

Symptom

The synchronization process failed to synchronize IBM Information Integrator for Content users with the MQ Workflow server using EIPUser2WF.bat. When you review the log file (temp.log), it shows output similar to the following example:

```
6/2/2004 1:29:18 PM FMC25100I CREATE PERSON 'CMB_U656' finished.
6/2/2004 1:29:18 PM FMC25100I CREATE PERSON 'CMB_U6560' finished.
6/2/2004 1:29:18 PM Assertion failed: 0 <= yy_ref_stack_ix && yy_ref_stack_ix
< yy_ref_stack_max, file e:\v340\src\yy_ref.h, line 354
```

Possible cause

The IBM Information Integrator for Content system administration database includes more than 5000 users.

Action

Manually subdivide the list of users and synchronize them with the MQ Workflow server in stages.

1. Open the temp.fdl and temp.log files. On Windows, both files are located in the *IBMCMROOT* directory. On AIX or Solaris, both files are located in the HOME directory.
2. Use the temp.log file to locate the last user that synchronized correctly. In the example output, the last successfully synchronized user is CMB_U6560.
3. In the temp.fdl file, delete every entry after the last successfully synchronized user. For example, the end of the file might show the following output:

```
PERSON 'CMB_U6560'
DESCRIPTION " Updated by EIPUser2WF EIP utility user CMB_U6560 "
PERSON_ID 'CMB_U6560'
AUTHORIZED_FOR STAFF
AUTHORIZED_FOR PROCESS_CATEGORY 'EIPMQSWF'
PASSWORD 'DOEaV8872'
GROUP 'FMCGRP'
SYSTEM 'FMCSYS'
IS_NOT_ABSENT
DO_NOT_RESET_ABSENT
END 'CMB_U6560'
```

4. Save this edited file as part1.fdl.

5. Open the original temp.fdl file again.
6. Leave the first three lines of the file intact and delete all entries up to and including the last successfully synchronized user (CMB_U6560 in the example). For example, the edited file might look like this example:

```
//Generated by EIP
CODEPAGE 1252
FM_RELEASE V3R4 0
PERSON 'CMB_U6561'
DESCRIPTION " Updated by EIPUser2WF EIP utility user CMB_U6561 "
PERSON_ID 'CMB_U6561'
AUTHORIZED_FOR STAFF
AUTHORIZED_FOR PROCESS_CATEGORY 'EIPMQSWF'
PASSWORD 'DOEaV8873'
GROUP 'FMCGRP'
SYSTEM 'FMCSYS'
IS_NOT_ABSENT
DO NOT RESET_ABSENT
END 'CMB_U6561'
...
```

Tip: If you are using MQ Workflow 3.3.2, you must manually adjust the MQ Workflow release level from FM_RELEASE V3R4 0 to FM_RELEASE V3R3 0.

7. Save the edited file as part2.fdl.
8. Enter the following command for each of the FDL files. The following example assumes that the MQ Workflow system administrator user ID is ADMIN and password is password.


```
* fmcibie -i part1.fdl -u admin -p password -o -l part1.log
* fmcibie -i part2.fdl -u admin -p password -o -l part2.log
```
9. Examine the log files to ensure that the synchronization completed without errors.

Failure to create workflow or retrieve workflow template

A failure to create workflow or retrieve workflow template might be because the wrong name was entered.

Symptom

You receive one of the following messages when starting workflows with the APIs:

DGL2474A: Fail to retrieve a workflow template

DGL2448A: Fail to create workflow

Possible cause

You might have specified the wrong name for the workflow template. The DKWorkflowFed *add* function is case-sensitive.

Action

Ensure that the name you gave for the advanced workflow template is the same as the name given to the advanced workflow template defined in the administration client.

Icon is reset each time the icon is dropped on the drawing surface in the workflow builder

If the icon is being reset each time that it is dropped on the drawing surface of the workflow builder, you should check your user preferences.

Symptom

The selection of an icon is reset each time that the icon is dropped on the drawing surface in the IBM Content Manager workflow builder.

Cause

The user preference for drawing preferences defaults to non-sticky mode.

Action

When creating a workflow diagram in the IBM Content Manager workflow builder, click **Edit commands > User preferences > Toolbar tab**. Select **Sticky** as the drawing preference. This selection is remembered for the life of the workflow diagram, but not for the workflow builder.

Workflow builder does not have work node variables listed in the Decision Point window

Problems with work node variables could be related to where they are defined in the workflow.

Symptom

The **Work node variables** radio button is clicked, but the **Variable** list, **Operator** list, and **Value** field are disabled and cannot be selected.

Cause

This problem can occur if there are no work node variables defined for the work nodes preceding the decision point node, or if work node variables are defined but the work nodes have not been connected to the decision point node.

For example, you might be creating a process with `work_node1` and `work_node2`. These work nodes have work node variables defined, but the connection has not been completed from `work_node2` to the decision point node. Therefore, the Decision Point window is not aware of `work_node1` and `work_node2` and any variables that might be defined for those nodes.

Action

For work node variables to be listed in the Decision Point window, define work node variables in the work nodes that precede the decision point node. Then connect those work nodes to the decision point node.

Incorrect routing of first document in a workflow

The first work package in a workflow can take an incorrect path through a decision point.

Symptoms

It is possible for a work package to take the wrong branch through a decision point. This problem occurs only if the decision is based on an item type for which only the first item is in the work package.

Resolving the problem

After the second item is stored, the problem does not occur.

Document routing performance problems during updates

When you update a document routing process, you can improve performance by indexing the ICMUT00204001 table.

Symptoms

When you update an IBM Content Manager document routing process, you might experience a performance problem such as the update running slowly.

Causes

This problem might be caused by many work packages in the system.

Diagnosing the problem

To check for the number of work packages in the system, run the following the SQL statement, where *ICMADMIN* is the schema of the library server database:

```
SELECT COUNT(*) FROM ICMADMIN.ICMUT00204001
```

If the count is large, the query to table ICMUT00204001 is probably causing the performance problem. The definition of a large number of work packages is determined by the processing speed and available memory on the machine where the library server is running.

Resolving the problem

To improve the query performance, you can manually create the index on the PROCESSITEMID column in the ICMUT00204001 table. To create the index for the library server database table ICMUT00204001:

- 1. Run one of the following sets of commands to create the index, where *CREATOR* is the library server administrator ID.

Table 88. Commands to create the index for ICMUT00204001

Database type	Commands
Content Manager EE with DB2	<pre>CREATE INDEX CREATOR.ICMUXUT002040023X ON CREATOR.ICMUT00204001 (PROCESSITEMID ASC) COLLECT DETAILED STATISTICS</pre>

Table 88. Commands to create the index for ICMUT00204001 (continued)

Database type	Commands
Content Manager EE with Oracle	<p>In this example, <i>ICM_LS_DBICMLSNDX</i> is the default index table space.</p> <pre> CREATE INDEX CREATOR. ICMUT002040023X ON CREATOR. ICMUT00204001 (PROCESSITEMID ASC) TABLESPACE ICM_LS_DBICMLSNDX COMPUTE STATISTICS </pre>
Content Manager for z/OS with DB2	<p>In this example, <i>STOGROUP</i> is the name defined for the DB2 storage group, <i>PRIINDX</i> is the name defined as the primary allocation amount for small table spaces, <i>SECINDX</i> is the name defined as the secondary allocation amount for small table spaces, and <i>BPV4</i> is the buffer pool name defined for library server indexes:</p> <pre> CREATE INDEX CREATOR. ICMUT002040023X ON CREATOR. ICMUT00204001 (PROCESSITEMID ASC) USING STOGROUP STOGROUP PRIQTY PRIINDX SECQTY SECINDX BUFFERPOOL BPV4 </pre>

- For z/OS, you must run the **runstat** command to update statistics for ICMUT00204001.

Locale-specific considerations

Review the locale-specific considerations for more information about how different locales can affect the configuration of a content management system.

The following troubleshooting topics apply to non-English systems in general:

- “Information center topics display in English” on page 572
- “Attribute sizing and string length considerations for non-English environments” on page 593
- “Problems with the LDAP import utility schedule on non-English Windows operating systems” on page 669

In addition to the general troubleshooting information provided in other sections, there are administration considerations and limitations that apply to specific languages and locales:

“Considerations for Lithuanian locale”

“Considerations for Thai locale” on page 682

“Considerations for Turkish locale” on page 682

Considerations for Lithuanian locale

Review the special instructions for full-text indexing in the Lithuanian locale.

Euro symbol cannot be indexed

For full-text indexing in IBM Content Manager, the Euro sign in Lithuanian-language documents cannot be indexed. Instead, you can conduct text search for the Euro sign for resource items or text search-enabled attributes.

Considerations for Thai locale

Review the special instructions for fonts and character display in the Thai locale.

Requirement: font installation

If the keyboard language and regional settings are configured to display Thai characters, but the text entered in a text field does not display the characters clearly, you must install a font. The necessary font is not included in the IBM Java Runtime Environment (JRE) provided with IBM Content Manager. The font is provided in the IBM Java Development Kit (JDK).

Copy the file `thonburi.ttf` from `JAVA_HOME\jre\lib\font` to `IBMCMROOT\java\jre\lib\fonts`.

Related reference

“Specifying code pages for phrased text search of Thai language content” on page 613

Considerations for Turkish locale

For the Turkish locale, rules about the lowercase letter *i* character affect some settings in your content management system.

Requirement: set IBM_CM_DISABLE_SACP

Because of the way the letter *i* is handled in Java for the Turkish locale, you must set the following system variable before running the system administration client: `IBM_CM_DISABLE_SACP=TRUE`.

If the `IBM_CM_DISABLE_SACP` variable is not set to true, you might receive the following error message when logging on to the system administration client:

```
No suitable driver(STATE): 08001(STATE):08001
```

Recommendation: use uppercase user IDs

Because there are multiple versions of the *i* character in Turkish, the name of IBM Content Manager objects used for administration (for example: schema name, user name, item types, attributes, and others) should be created with uppercase characters. IBM Content Manager converts the name of these objects to uppercase characters internally, and objects for administration named with a lowercase *i* character do not work.

Related reference

“Specifying code pages for phrased text search of Thai language content” on page 613

Setting up your system to integrate with FileNet Business Process Manager

To prepare your system for FileNet Business Process Manager integration, you must complete several administration tasks.

Before you begin the tasks for setting up your system, ensure that you have all of the required products and components.

Setting up your system for FileNet Business Process Manager integration includes setting up the Java Message Service (JMS) for WebSphere MQ, setting up the connection to FileNet Business Process Manager, working with the event monitor and event handler, and subscribing to events.

“FileNet Business Process Manager integration”

“Configuring the library server for an Oracle system” on page 687

“Setting up a JMS queue in WebSphere MQ” on page 688

“Setting up a JMS queue in WebSphere MQ with LDAP” on page 690

“Setting up the FileNet Business Process Manager connection” on page 693

“Modifying the event monitor and event handler settings” on page 696

“Starting and stopping the event monitor” on page 698

“Starting and stopping the event handler” on page 700

“Subscribing to events” on page 701

Related reference

 Required software

Related information

System Administration Client and z/OS

Installing FileNet Business Process Manager

Updating your content management system from Version 8.4.1 to Version 8.4.2

Upgrading your content management system from Version 8.3 to Version 8.4.2

FileNet Business Process Manager integration

You can integrate IBM Content Manager with FileNet Business Process Manager by enabling your IBM Content Manager objects for FileNet Business Process Manager.

The integration of IBM Content Manager with FileNet Business Process Manager includes the following features:

- An automatic start of one or more FileNet Business Process Manager processes when a configured type of content is added or updated within IBM Content Manager.

For example, an IBM Content Manager item type is configured for use with FileNet Business Process Manager by associating the events that can occur on that item type with a FileNet Business Process Manager process. This association is known as an event subscription. When a document of that item type has an action performed on it, such as document creation in IBM Content Manager, then FileNet Business Process Manager is called to start a new process with this document as an attachment. Different actions on a document in this item type

can trigger different FileNet Business Process Manager processes, based on the associations that are made in the event subscription.

- A set of component integrator functions for IBM Content Manager. The Component Integrator is a FileNet Business Process Manager extensible integration framework that enables a workflow to connect with an external system. The component integrator functions for IBM Content Manager are in the `DKContentOperationsICM` class.
- A way for administrators to configure IBM Content Manager servers to integrate with FileNet Business Process Manager.

The following diagram shows the component architecture of a system that integrates IBM Content Manager with FileNet Business Process Manager.

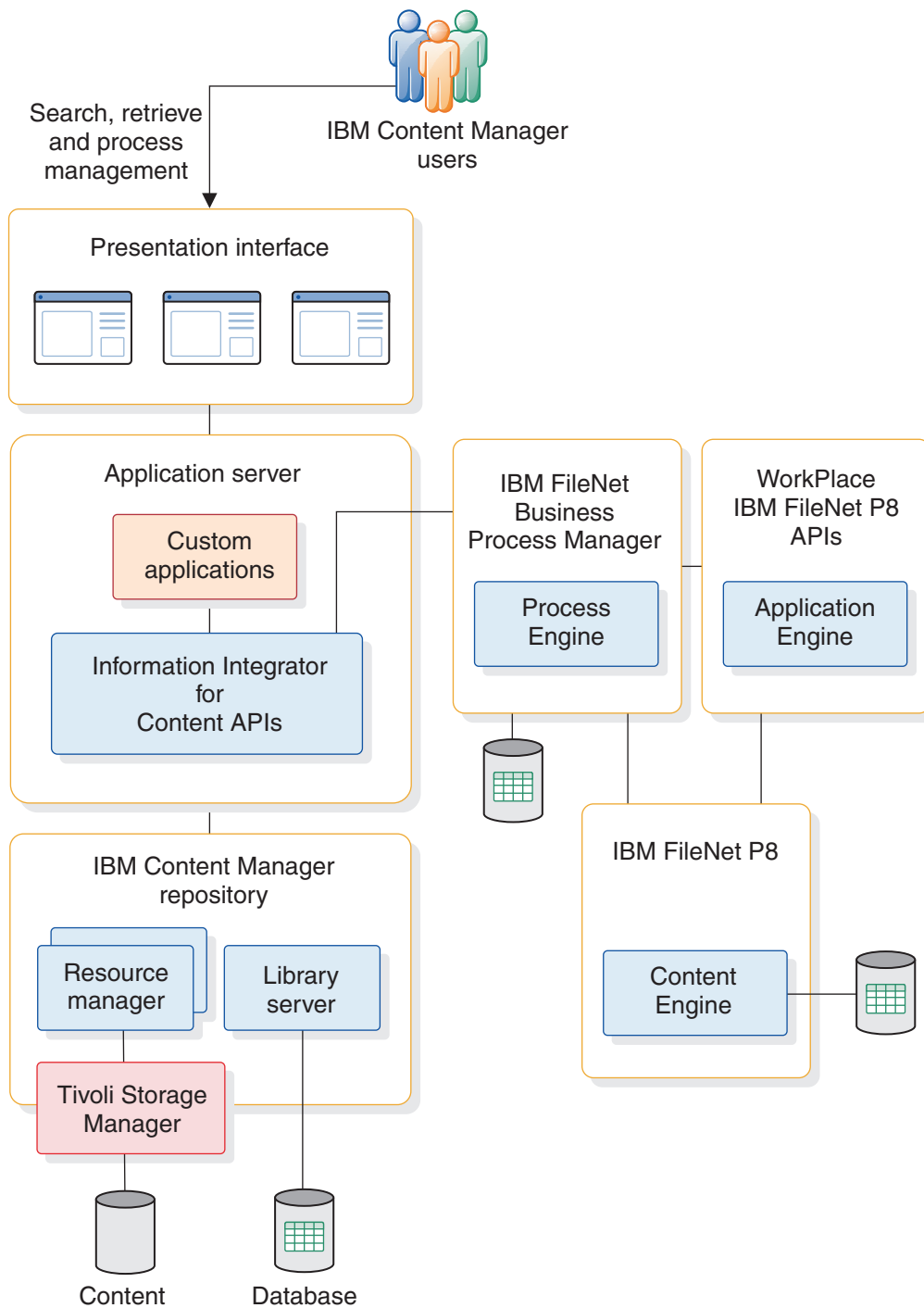


Figure 30. Architectural overview of the FileNet Business Process Manager integration with IBM Content Manager

“Example system configuration with FileNet Business Process Manager” on page 686

Related information

 [developerWorks: An event-driven framework for integrating IBM Content Manager with IBM FileNet Business Process Manager](#)

Example system configuration with FileNet Business Process Manager

To connect IBM Content Manager with FileNet Business Process Manager, you must install and configure the components that enable the integration between the two systems.

The following components enable the integration between IBM Content Manager and FileNet Business Process Manager:

LDAP server

Ensures that FileNet Business Process Manager users have the proper access to IBM Content Manager items.

Event monitor

Monitors IBM Content Manager library server events to determine which item type events can start a FileNet Business Process Manager process.

Event handler

Processes IBM Content Manager events to extract the Common Base Event (CBE) formatted event and calls the FileNet Business Process Manager process based on the event data.

MQ server

Provides Java Message Service (JMS) support for the event monitor and event handler.

The following diagram is an example system configuration that shows how these components work together to integrate IBM Content Manager with FileNet Business Process Manager. The configuration that is shown is not the only way to integrate these components. Other example configurations include installing all components on a single machine, installing all IBM Content Manager components on a single machine and all FileNet Business Process Manager components on a single machine, or installing each component on a different machine for an installation that is as distributed as possible. See the *Planning and Installing Guide* for more information about planning for a FileNet Business Process Manager installation.

The IBM Content Manager installation program creates the large object (LOB) columns in the same table space as the ICMSTEVENTQUEUE table, a setup that can decrease performance. To ensure that you do not have performance problems, you must create a new table space and move the EVENTDATAC and EVENDATAB LOB columns to the new table space.

To create a new table space and move the columns:

1. Create a new table space by issuing the following commands:

```
CREATE TABLESPACE ICML0BCOL04
DATAFILE 'icml0bcol04.dat' SIZE 200M
REUSE ONLINE NOLOGGING
DEFAULT STORAGE (MAXEXTENTS UNLIMITED)
```

2. Move the columns to the new table space by issuing the following commands:

```
ALTER TABLE ICMSTEVENTQUEUE
MOVE LOB(EVENTDATAC, EVENDATAB) STORE AS
( TABLESPACE ICML0BCOL04
  DISABLE STORAGE IN ROW
  CHUNK 32768
  PCTVERSION 0
  NOCACHE NOLOGGING
  STORAGE (INITIAL 10M NEXT 10M
  MAXEXTENTS UNLIMITED
  PCTINCREASE 0)
)
```

3. Determine whether you need to rebuild the primary key of the ICMSTEVENTQUEUE table. If the table had data when you issued the MOVE LOB command in the previous step, you must rebuild the primary key of the ICMSTEVENTQUEUE table. To verify that you must rebuild the primary key, run the following query:

```
SQL> SELECT STATUS, INDEX_NAME FROM ALL_INDEXES WHERE
TABLE_NAME='ICMSTEVENTQUEUE';
```

If the query returns a status of UNUSABLE as in the following example, you must rebuild the primary key.

```
STATUS    INDEX_NAME
-----
UNUSABLE  SYS_C003085
```

4. Optional: To rebuild the primary key, run the following command by using the *index_name* value from the previous step:

```
SQL> ALTER INDEX SYS_C003085 REBUILD;
Index altered
```

Setting up a JMS queue in WebSphere MQ

You must set up a Java Message Service (JMS) queue to act as a message staging area for the event monitor and handler.

Ensure that WebSphere MQ is properly installed and configured.

The information in this task provides general reference information. For complete information, see the JMS setup procedures in the WebSphere MQ documentation.

You can use either the file system context or the LDAP context to configure your WebSphere MQ JMS for the event monitor and handler. The file system context is the default setting for the WebSphere MQ JMS configuration, and it does not provide any security mechanism to prevent unauthorized access to the JMS queue. The LDAP context provides LDAP authentication to protect the JMS queue from unauthorized access.

To set up a JMS queue with the file system context:

1. In WebSphere MQ, start the WebSphere MQ Explorer.
2. Create a queue manager and make it the default queue manager. For example, create QM_myhost.
3. Create a local queue in the queue manager. For example, create BPMQueue.
4. In a text editor, open the JMSAdmin.config file from the /bin directory of the WebSphere MQ JMS installation directory. Remove the comment symbols from the following entries to define the file system context with the appropriate values:

INITIAL_CONTEXT_FACTORY=com.sun.jndi.fscontext.ReffFSContextFactory

The file system context factory.

PROVIDER_URL=file://C:/jndi

The provider URL of the file system context.

The following example shows a portion of the JMSAdmin.config file with the file system context defined:

```
#INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
INITIAL_CONTEXT_FACTORY=com.sun.jndi.fscontext.ReffFSContextFactory
#INITIAL_CONTEXT_FACTORY=com.ibm.ejs.ns.jndi.CNInitialContextFactory
#INITIAL_CONTEXT_FACTORY=com.ibm.websphere.naming.WsnInitialContextFactory
#
# The following line specifies the URL of the service provider's initial
# context. It currently refers to an LDAP root context. Examples of a
# file system URL and WebSphere's JNDI namespace are also demonstrated,
# but commented out.
#
#PROVIDER_URL=ldap://polaris/o=ibm,c=us
#PROVIDER_URL=file://C:/JNDI-Directory
#PROVIDER_URL=iiop://localhost/
PROVIDER_URL=file://C:/JNDI
#
```

5. Start the JMS administration tool by running the following command:
JMSADMIN -t -v -cfg JMSADMIN.config
6. Define the queue connection factory by running the following command, where QCFactory is an example queue connection factory name:

```
define QCF(QCFactory)
```

7. Define a JMS queue that is based on a physical queue in the default queue manager by running the following command, where ICMMSGOQ is an example JMS queue name:

```
define Q(ICMMSGOQ) QUEUE(BPMQueue)
```

8. Optional: Display the JMS queue information by running the following command:

```
display ctx
```

The output appears as follows, where ICMMSGOQ is the JMS queue name and QCFactory is the queue connection factory name:

Contents of InitCtx

```
.bindings          java.io.File
a ICMMSGOQ          com.ibm.mq.jms.MQQueue
a QCFactory         com.ibm.mq.jms.MQQueueConnectionFactory

3 Object(s)
0 Context(s)
3 Binding(s), 2 Administered
```

9. Run the WebSphere MQ JMS utility for system queues by running the following command:

```
runmqsc < MQJMS_PSQ.mqsc
```

Related information

 WebSphere MQ, Version 6.0

Setting up a JMS queue in WebSphere MQ with LDAP

You must set up a Java Message Service (JMS) queue to act as a message staging area for the event monitor and handler.

Ensure that WebSphere MQ is properly installed and configured. The LDAP server must be available, and users must be defined before you configure the JMS queue.

The information in this task provides general reference information. For complete information, see the JMS setup procedures in the WebSphere MQ documentation.

You can use either the file system context or the LDAP context to configure your WebSphere MQ JMS for the event monitor and handler. Use the LDAP context setting for the WebSphere MQ JMS configuration with LDAP authentication. The file system context is the default, but it does not provide any security mechanism to prevent unauthorized access to the JMS queue. The LDAP context provides LDAP authentication to protect the JMS queue from unauthorized access.

To set up a JMS queue with the LDAP context:

1. In WebSphere MQ, start the WebSphere MQ Explorer.
2. Create a queue manager and make it the default queue manager. For example, create QM_myhost.
3. Create a local queue in the queue manager, for example, BPMQueue.
4. In a text editor, open the JMSAdmin.config file from the /bin directory of the WebSphere MQ JMS installation directory. Remove the comment symbols from the following entries to define the LDAP context with appropriate values:

INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory

The LDAP context factory.

PROVIDER_URL=ldap://localhost/o=IBM,c=US

The LDAP server and context.

SECURITY_AUTHENTICATION=simple

Simple authentication mode.

PROVIDER_USERDN=cn=root

User distinguished name.

PROVIDER_PASSWORD=password

Password for the user distinguished name.

USE_INITIAL_DIR_CONTEXT=TRUE

Initial directory context.

The following example shows the a portion of the JMSAdmin.config file with the LDAP context defined:

```
# -----  
# IBM Websphere MQ Support for Java Message Service  
# This is the default configuration file for the Websphere MQ Classes for  
# Java Message Service Administration Tool.  
#  
# %PUB_START%  
# Licensed Materials - Property of IBM  
#
```

```

# 5724-H72, 5655-L82, 5724-L26
#
# (c) Copyright IBM Corp. 2002, 2005
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# %PUB_END%
# -----
#
# The following line specifies which JNDI service provider is in use.
# It currently indicates an LDAP service provider. If a different
# service provider is used, this line should be commented out and the
# appropriate one should be uncommented.
#
INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
#INITIAL_CONTEXT_FACTORY=com.sun.jndi.fscontext.ReffFSContextFactory
#INITIAL_CONTEXT_FACTORY=com.ibm.ejs.ns.jndi.CNInitialContextFactory
#INITIAL_CONTEXT_FACTORY=com.ibm.websphere.naming.WsnInitialContextFactory
#
# The following line specifies the URL of the service provider's initial
# context. It currently refers to an LDAP root context. Examples of a
# file system URL and WebSphere's JNDI namespace are also shown, commented
# out.
#
PROVIDER_URL=ldap://localhost/o=IBM,c=US
#PROVIDER_URL=file:/C:/JNDI-Directory
#PROVIDER_URL=iiop://localhost/
#PROVIDER_URL=file:///C:/jndi
#
# The following line specifies the security authentication model in use,
# and may be 'none' (for anonymous authentication), 'simple', or 'CRAM_MD5'.
#
SECURITY_AUTHENTICATION=simple
#
# If you don't have SECURITY_AUTHENTICATION=none, then JMSAdmin will
# prompt you for the User DN and password. If you want to bypass these
# prompts then you can specify one or both of the values here. Since
# the password here is in cleartext this is not normally recommended
# except for testing. You should replace these values with your own.
#
PROVIDER_USERDN=cn=root
PROVIDER_PASSWORD=password
#
#
# The following line determines whether to use an InitialDirContext, or an
# InitialContext. Takes value of TRUE or FALSE.
USE_INITIAL_DIR_CONTEXT=TRUE
#
#

```

5. Start the JMS administration tool by running the following command:
`JMSADMIN -t -v -cfg JMSADMIN.config`
6. Define the queue connection factory by running the following command, where QCFactory is an example queue connection factory name:
`define QCF(QCFactory)`
7. Define a JMS queue that is based on a physical queue in the default queue manager by running the following command, where ICMMSGOQ is an example JMS queue name:
`define Q(ICMMSGOQ) QUEUE(BPMQueue)`
8. Optional: Display the JMS queue information by running the following command:
`display ctx`

The output appears as follows for a Tivoli Directory Server environment, where ICMMSGOQ is the JMS queue name and QCFactory is the queue connection factory name:

Contents of InitCtx

```
[D] ou=Sales                javax.naming.directory.DirContext
[D] ou=Groups               javax.naming.directory.DirContext
[D] ou=Finance              javax.naming.directory.DirContext
  a cn=QCFactory            com.ibm.mq.jms.MQQueueConnectionFactory
  a cn=ICMMSGOQ             com.ibm.mq.jms.MQQueue

5 Object(s)
  3 Context(s)
  2 Binding(s), 2 Administered
```

The output appears as follows for a Microsoft Windows Server Active Directory 2003 environment:

Contents of InitCtx

```
...
[D] CN=icmadmin             javax.naming.directory.DirContext
[D] CN=icmadmin1            javax.naming.directory.DirContext
[D] CN=icmconct             javax.naming.directory.DirContext
  a CN=ICMMSGOQ             com.ibm.mq.jms.MQQueue
  a CN=QCFactory            com.ibm.mq.jms.MQQueueConnectionFactory
...

52 Object(s)
  50 Context(s)
  2 Binding(s), 2 Administered
```

9. Run the WebSphere MQ JMS utility for system queues by running the following command:

```
runmqsc < MQJMS_PSQ.mqsc
```

"LDAP server configuration for storing Java objects"

Related information



WebSphere MQ, Version 6.0

LDAP server configuration for storing Java objects

Before you set up the JMS queue, you might need to configure your LDAP server for storing Java objects to support the RFC 2713 schema.

WebSphere MQ and the Java Message Service (JMS) require the LDAP provider to store the JMS context information as Java objects. Some LDAP providers, such as Microsoft Active Directory, might require additional configuration to support RFC 2713: Schema for Representing Java Objects in an LDAP Directory. This schema defines elements to represent a Java serialized object, a Java marshalled object, and a Java Naming and Directory Interface (JNDI) reference. A Java remote object is stored as either a Java marshalled object or a JNDI reference.

Sun Microsystems provides a Java tool, CreateJavaSchema, to configure the schema for storing Java objects for JMS. You can download a complete compressed file from the Sun Microsystems JNDI LDAP service provider Web site. You can also find additional information in the WebSphere MQ documentation.

If the directory's administration tool supports the disabling of schema checking, turn off schema checking before running the CreateJavaSchema tool as recommended in the CreateJavaSchema tool's instructions.

Example

Follow this Microsoft Windows Server Active Directory 2003 example to run the CreateJavaSchema tool. Enter the following command, where *ldap://www.myhost.com* is the LDAP server URL, *cmuser* is the distinguished name for authentication, and *password* is the password for authentication:

```
java -Djava.naming.provider.url=ldap://www.myhost.com
CreateJavaSchema -sad -ncmuser -ppassword
```

The tool displays output that is similar to the following example:

```
[updating Active Directory schema ...]
[locating the schema]
[inserting new attribute definitions ...]
[javaClassName]
[javaCodeBase]
[javaSerializedData]
[javaFactory]
[javaReferenceAddress]
[javaDoc]
[javaClassNames]
[inserting new object class definitions ...]
[javaContainer]
[javaObject]
[javaSerializedObject]
[javaNamingReference]
[javaMarshaledObject]
[update completed]
Use your directory server's administration tool to verify
that the schema is correct:
```

Tip:

If you use Microsoft Windows Server Active Directory 2003, use the `-sad` option for the CreateJavaSchema command as shown in this example to work around schema bugs in the server. Also, to enable any schema modifications, you must create the Schema Update Allowed registry property of type **DWORD** and set the value to 1. Open the registry editor and create this registry property in the following location: **HKEY_LOCAL_MACHINE > System > CurrentControlSet > Services > NTDS > Parameters > Schema Update Allowed**.

Related reference

 [Sun Java Naming and Directory Interface \(JNDI\)](#)

Related information

 [RFC 2713: Schema for Representing Java Objects in an LDAP Directory](#)

 [Sun Microsystems Web site](#)

 [WebSphere MQ, Version 6.0](#)

Setting up the FileNet Business Process Manager connection

Set up the connection to FileNet Business Process Manager in the IBM Content Manager system administration client to enable the client to display Business Process Manager data in system administration client fields. If you set up this connection, then Business Process Manager workflow process names and workflow process attributes display when you configure process integration event subscriptions.

When you set up the Business Process Manager connection, you configure a host name, port number, and connection point for FileNet Business Process Manager in the IBM Content Manager system administration client. This data enables IBM Content Manager to construct a bootstrap URL to connect to Business Process Manager.

After you configure the data used for the bootstrap URL, you log on to the Business Process Manager server to verify that the setup is correct.

“Configuring the FileNet Business Process Manager connection in the system administration client”

“Logging on to FileNet Business Process Manager” on page 695

Configuring the FileNet Business Process Manager connection in the system administration client

Configure a host name, port number, and connection point for FileNet Business Process Manager in the IBM Content Manager system administration client to enable IBM Content Manager to construct a bootstrap URL to connect to FileNet Business Process Manager.

During the installation and configuration of the system administration client, you can set up the connection to FileNet Business Process Manager. If you did not set up the connection during a new installation or upgrade of IBM Content Manager, then you can use the steps in this procedure to set up the connection. Setting up the connection to FileNet Business Process Manager enables the system administration client to display FileNet Business Process Manager workflow process names and workflow process attributes during the configuration of process integration event subscriptions.

To configure the FileNet Business Process Manager connection, you supply the host name and port number of the FileNet Content Engine application server. You can find these settings in the `WcmAPIConfig_wsi.properties` properties file for the Content Engine. This file is located in the following path: `%IBMCMROOT%\P8Client\CEClient\`. You can also contact the Content Engine administrator for additional information.

The host name and port number that you supply in the configuration data set up the Java Virtual Machine (JVM) properties to construct the bootstrap URL. The following example shows how these values are used, where *fully_qualified_hostname* is the fully qualified host name of the FileNet Content Engine application server and *port_number* is the port number of the FileNet Content Engine application server: `http://fully_qualified_host_name:port_number/WSI/FNCEWS40MTOM/`. This bootstrap URL enables the IBM Content Manager system administration client to log on to FileNet Business Process Manager.

Tip: When you are configuring this connection, you can also select an option to create a secure URL with an `https://` prefix if your Content Engine uses Secure Sockets Layer (SSL) as a security protocol.

To configure the FileNet Business Process Manager connection, you also supply the connection point for the FileNet Process Engine. This connection point is also known as the PE Connection Point. The PE Connection Point is set in the Content Engine administration tool, the FileNet Enterprise Manager. If you need additional information about where to find the connection point, contact your Content Engine administrator.

To configure the FileNet Business Process Manager connection in the system administration client:

1. From the system administration client, click **Tools > FileNet Business Process Manager Configuration**.
2. In the **Fully qualified host name** field, enter the fully qualified host name of the FileNet Content Engine application server.
3. In the **Bootstrap port number** field, enter the port number of the FileNet Content Engine application server.
4. In the **Connection point** field, enter the FileNet Process Engine connection point.
5. If your Content Engine is configured to SSL, select **FileNet Content Engine configured to use Secure Sockets Layer (SSL)**. Selecting this check box creates a secure URL with the `https://` prefix instead of the `http://` prefix. Click **OK** to save the configuration.

Related tasks

Logging on to FileNet Business Process Manager

Logging on to FileNet Business Process Manager

After you configure the connection to FileNet Business Process Manager in the system administration client, or when you create an event subscription, the system administration client might display a dialog box to log on to FileNet Business Process Manager.

After you configure the connection data for FileNet Business Process Manager, the system administration client attempts to log on to FileNet Business Process Manager to verify the configuration. By default, the system administration client uses the ID and password of the IBM Content Manager system administrator that is currently logged on to the system administration client. If that ID and password does not match the user name and password for FileNet Business Process Manager, then you must log on with the correct FileNet Business Process Manager information. The system administration client opens the FileNet Business Process Manager Logon window for you to enter the user name and password. The FileNet Business Process Manager uses the FileNet Content Engine for authentication, so you must enter the user name and password for the FileNet Content Engine.

If you configured the connection to FileNet Business Process Manager, then the first time that you create an event subscription during a system administration client session, the system administration client also attempts to log on to FileNet Business Process Manager by using the current Content Manager EE administrator ID and password. If the logon attempt is not successful, the system administration client opens the FileNet Business Process Manager Logon window.

Recommendation: To reduce the amount of system administration client requests to log on to FileNet Business Process Manager, use the same user ID and password for the IBM Content Manager administrator and the FileNet Content Engine.

To log on to the FileNet Business Process Manager server:

1. In the **User Name** field, enter the user name to log on to FileNet Business Process Manager.
2. In the **Password** field, enter the password to log on to FileNet Business Process Manager.

Related tasks

Configuring the FileNet Business Process Manager connection in the system administration client

Modifying the event monitor and event handler settings

You can modify the event monitor and event handler settings by modifying the parameters in the `cmbemconfig.properties` file.

The settings for the event monitor and event handler are configured in the `cmbemconfig.properties` file. You might want to modify these settings. For example, during performance tuning you might find that modifying the scan interval setting on the event monitor improves performance, based on your system resources.

To complete this task, you must edit the `cmbemconfig.properties` file, which is in the following subdirectory of the IBM Content Manager working directory:

Windows

`cmgmt\em`

UNIX `cmgmt/em`

Tip: You can also modify a subset of the parameters in the `cmbemconfig.properties` file by running the configuration wizard for IBM Information Integrator for Content. The subset of the parameters that you can modify by running this configuration wizard includes the following parameters:

- `INITIAL_CONTEXT_FACTORY`
- `PROVIDER_URL`
- `QUEUE_CONNECTION_FACTORY`
- `QUEUE_NAME`
- `EH_LOG_FILE`
- `FILENET_LOGIN_CONFIG`
- `FILENET_WASP_LOCATION`
- `FILENET_CEURI`
- `FILENET_CONN_PT`
- `LDAP_BASE_DN`
- `LDAP_PREFIX`

The example settings are for a Windows environment. If you are using a UNIX environment, you must modify the values accordingly.

To modify the event monitor and event handler settings:

1. Open the `cmbemconfig.properties` file in a text editor and modify the following parameters as appropriate:

Table 89. LDAP settings that are common to both the event monitor and event handler

Parameter name	Definition	Sample value
<code>LDAP_BASE_DN</code>	The Lightweight Directory Access Protocol (LDAP) base distinguished name (DN). This setting is optional and applicable in an LDAP context only. The base DN is used to construct an LDAP principal.	<code>CN=Users,DC=svl,DC=ibm,DC=com</code>
<code>LDAP_PREFIX</code>	The default LDAP prefix. This setting is optional and is applicable in an LDAP context only.	<code>cn=</code>

Table 90. Java Message Service (JMS) settings that are common to both the event monitor and event handler

Parameter name	Definition	Sample value
INITIAL_CONTEXT_FACTORY	The Java Naming and Directory Interface (JNDI) context factory.	For the file system context: com.sun.jndi.fscontext.RefFSContextFactory For the LDAP context: com.sun.jndi.ldap.LdapCtxFactory
PROVIDER_URL	The URL of the provider.	For the file system context: file://c:/jndi For the LDAP context, the URL pointing to an LDAP server: PROVIDER_URL=ldap://localhost/o=IBM,c=US
QUEUE_CONNECTION_FACTORY	The name of the queue connection factory.	QCFactory
QUEUE_NAME	The name of the queue.	ICMMSGOQ

Table 91. Event monitor settings

Parameter	Definition	Sample value
SCAN_INTERVAL	The default scan interval, in seconds, that defines how frequently the event monitor scans the event table for events. If you enter a scan interval value of 0, the scan cycle will continue without any delay. Recommendation: A scan interval set to 0 can consume excessive system resources. For performance reasons, do not enter a value of 0.	60
PURGE_INTERVAL	The default purge interval, in seconds, that defines how frequently the event monitor purges processed events from the event table. If you enter a purge interval value of 0, the purge cycle will continue without any delay. An example value is 300. Recommendation: A purge interval set to 0 can consume excessive system resources to maintain a constant purge cycle. For performance reasons, do not enter a value of 0.	300
EXPIRATION_TIME	The expiration time of a JMS message in hours. The message is removed from the JMS queue when the expiration time is reached. If you enter an expiration time with a value of 0, the message stays in the JMS queue until it is consumed by the event handler or removed by an administrator. Recommendation: An expiration time set to 0 can cause the JMS queue to become larger than recommended. Do not enter a value of 0.	48
SCAN_SIZE	The default scan size per scan interval. The scan size is the limit for the number of events found in a scan. If you set this value to 0, all unprocessed library server events are retrieved. Recommendation: A scan size set to 0 can consume excessive system resources to retrieve every unprocessed event. For performance reasons, do not enter a value of 0.	100
DUMP_EM_CFG	The setting to write the event monitor configuration data from the event monitor to the log file (icmmonitor.log).	To turn the setting on: 1 To turn the setting off: 0
DUMP_EM_EVT	The setting to write event data from the event monitor to the log file (icmmonitor.log).	To turn the setting on: 1 To turn the setting off: 0

Table 92. Event handler settings

Parameter	Definition	Sample value
RETRY_COUNT	The number of times for the event handler to retry starting a workflow.	3
EH_LOG_FILE	The file path for the event handler log file.	c:\\temp\\icmhandler.log
EH_LOG_LEVEL	The event handler logging level, such as ERROR or DEBUG.	ERROR
EH_LOG_MAXBACKUP	The number of error log files to back up.	5

Table 92. Event handler settings (continued)

Parameter	Definition	Sample value
EH_LOG_MAXSIZE	The maximum size of the log file. Enter this value as the integer and the unit of measurement, with no space between the integer and the unit. The values KB (for kilobytes), MB (for megabytes), and GB (for gigabytes) are valid units of measurement. Recommendation: For the optimum log file size, use megabytes (MB) as the unit of measurement.	1MB
FILENET_LOGIN_CONFIG	The Java Virtual Machine (JVM) parameter for specifying the login configuration file for -Djava.security.auth.login.config when connecting to an IBM FileNet server.	c:/progra~1/IBM/db2cmv8/P8Client/CEClient/config/jaas.conf.WSI
FILENET_WASP_LOCATION	The JVM parameter for specifying -Dwasp.location when connecting to an IBM FileNet server. This parameter is applicable only for FileNet Business Process Manager Version 4.5.0 and is not needed for Version 4.5.1.	c:/progra~1/IBM/db2cmv8/P8Client/CEClient/wsi
FILENET_CEURI	The JVM parameter for specifying the Uniform Resource Identifier (URI) for -Dfilenet.pe.bootstrap.ceuri. This value is the bootstrap URL that connects IBM Content Manager and FileNet Business Process Manager and includes the fully qualified host name and port number of the Content Engine.	http://www.example.com:9080/wsi/FNCEWS40MTOM/
FILENET_CONN_PT	The connection point for the Process Engine. A connection point defines a specific isolated region of the workflow database that is used by the Process Engine. You can find the list of available connection points on the Content Engine Enterprise Manager.	PECP
DUMP_EH_EVT	The setting to write event handler event data from the event handler to the log file (icmhandler.log).	To turn the setting on: 1 To turn the setting off: 0

- After you make the changes, save the cmbemconfig.properties file. Then, start the event monitor and the event handler again for the new settings to take effect.

Related tasks

“Starting and stopping the event handler” on page 700

“Starting and stopping the event monitor”

Monitoring and handling events

Starting and stopping the event monitor

The event monitor is a command-line utility that you must manually start to begin monitoring specified item type events.

Before you start the event monitor, ensure that you configured your Java Message Service (JMS) environment. Also ensure that you enabled the library server for event subscriptions in the library server configuration.

Only one instance of the event monitor can be running. To prevent more than one running instance of the event monitor, a flag in the library server is set every time that you start the event monitor. If the flag is set but the event monitor is not running, you can click the **Reset** button to clear the flag.

To start or stop the event monitor:

- Run one of the following commands:

Option	Command
Starting	ICMEvent -d <i>database_name</i> -u <i>user_id</i> [-s <i>schema_name</i>]

Option	Command
Stopping	QUIT

The `-s schema_name` parameter in the start command is an optional parameter. If you do not enter `-s schema_name` as part of the command, the event monitor uses the current user ID as the schema name.

Important:

On UNIX, part of the password might be displayed in the console if you edit the password by using the Backspace key. For password security reasons, avoid using the Backspace key when you edit the password.

On Windows, the password displays in the console when you press the Up Arrow key. The display of the password is caused by the command history function in Windows. To clear the command history after a password is entered, press ALT+ SHIFT+F7.

2. Enter the administrator LDAP principal and credentials if you are prompted. The event monitor checks the type of context factory in the property file. If the JMS is using the LDAP context `com.sun.jndi.ldap.LdapCtxFactory`, the authentication mechanism is enabled and you are prompted for the LDAP principal and credentials. Otherwise, if the JMS is using the file system context `com.sun.jndi.fscontext.RefFSCtxFactory`, no authentication is performed. The event monitor does not call the JNDI API with the LDAP principal and credentials to authenticate the user.

Important:

The following properties are required in the `cmbemlogconfig.properties` file for LDAP authentication:

LDAP_BASE_DN

The base distinguished name (DN) to use for the LDAP user. An example value is `CN=Users,DC=svl,DC=ibm,DC=com`.

LDAP_PREFIX

The prefix of an LDAP object. An example value is `cn=`.

To create a valid DN (distinguished name), the `LDAP_PREFIX` value is added as a prefix to the user name value. The `LDAP_BASE_DN` value, if specified, is appended after the user name value. The following list shows example values for each of these three parameters:

- The LDAP user name is `user1`.
- The `LDAP_BASE_DN` is `CN=Users,DC=svl,DC=ibm,DC=com`.
- The `LDAP_PREFIX` is `cn=`.

With those values set, the complete distinguished name is `cn=user1,CN=Users,DC=svl,DC=ibm,DC=com`.

A successful authentication allows the event monitor to obtain the JMS context objects, such as the queue connection factory objects and the queue object for establishing a valid connection to a JMS queue.

Related tasks

“Viewing or modifying the library server configuration” on page 6

Modifying the event monitor and event handler settings

Monitoring and handling events

Setting up a JMS queue in WebSphere MQ

Setting up a JMS queue in WebSphere MQ with LDAP

Starting and stopping the event handler

The event handler is a command-line utility that processes event information and starts a workflow in FileNet Business Process Manager.

You must have a FileNet Business Process Manager connection point and a FileNet Business Process Manager user ID and password to start the event handler.

To start or stop the event handler:

1. Run one of the following commands:

Option	Command
Starting	<code>ICMHandler -c <i>connection point</i> -u <i>user_id</i></code>
Stopping	<code>QUIT</code>

You must use a valid connection point and user ID so that the event handler can connect to the server.

Important:

On UNIX, part of the password might be displayed in the console if you edit the password by using the Backspace key. For password security reasons, avoid using the Backspace key when you edit the password.

On Windows, the password displays in the console when you press the Up Arrow key. The display of the password is caused by the command history function in Windows. To clear the command history after a password is entered, press ALT+ SHIFT+F7.

2. If you are prompted, enter the administrator LDAP principal and credentials. If the JMS is using the LDAP context `com.sun.jndi.ldap.LdapCtxFactory`, the authentication mechanism is enabled. The authentication mechanism requires that you provide the administrator LDAP principal and credentials. If the JMS is using the file system context `com.sun.jndi.fscontext.RefFSCtxFactory`, no authentication is performed.

Important:

The following properties are required in the `cmbemlogconfig.properties` file for LDAP authentication:

LDAP_BASE_DN

The base distinguished name (DN) to use for the LDAP user. Example: `CN=Users,DC=svl,DC=ibm,DC=com`.

LDAP_PREFIX

The prefix of an LDAP object. Example: `cn=`.

To create a valid DN (distinguished name), the LDAP_PREFIX value is added as a prefix to the user name value. The LDAP_BASE_DN value, if specified, is appended after the user name value. The following list shows example names for each of these three parameters:

- The LDAP user name is user1.
- The LDAP_BASE_DN is CN=Users,DC=svl,DC=ibm,DC=com.
- The LDAP_PREFIX is cn=.

With those values set, the complete distinguished name is
cn=user1,CN=Users,DC=svl,DC=ibm,DC=com.

The event handler calls the JNDI API with the LDAP principal and credentials that you provided to authenticate the user. A successful authentication allows the event handler to obtain the JMS context objects, such as queue connection factory objects and the queue object for establishing a valid connection to a JMS queue.

Related tasks

Modifying the event monitor and event handler settings

Monitoring and handling events

Subscribing to events

You can subscribe to events to enable the association of IBM Content Manager events with processes that occur in other applications.

“Event subscriptions”

“Enabling IBM Content Manager item types to start a FileNet Business Process Manager process with process integration” on page 702

“Defining an event subscription for general integration” on page 704

“Updating or deleting an event subscription” on page 704

Event subscriptions

An *event subscription* is an item type structure that associates an event that occurs on an item type with a process that occurs in another application. Event subscriptions can be used to start processes in other applications when events occur in IBM Content Manager.

When you create an item type, you can enable event subscriptions on the item type by using the system administration client. When an item type is enabled for event subscription, a library server event is generated every time that an item of that item type is created, deleted, or updated. The event monitor transforms the library server event to an IBM Content Manager event, packages the event in the Common Base Event (CBE) format as an XML string with the IBM Content Manager event, and sends the CBE formatted event to the event handler in the form of a Java Message Service (JMS) message.

You can enable two types of event subscriptions:

Process integration

An event subscription type that integrates with external workflow engines such as FileNet Business Process Manager. This type of event subscription enables IBM Content Manager to package event data with workflow related information such as process name, process data fields, and so on. When process integration is used, the event data includes a special integration code for FileNet Business Process Manager. The integration code is used by the built-in event handler provided by IBM Content

Manager to process the event and notify the correct application or engine to start the configured FileNet Business Process Manager process.

General integration

An event subscription type that integrates with external applications or engines other than workflow engines. When general integration is used, you must provide a custom event handler to process the event, send notifications to the external application or engine, and start the correct process. The code for this customized event handler must be able to discover which application to notify when an event is retrieved from the JMS queue.

Beginning with IBM Content Manager Version 8.4.3, a new event handler toolkit is packaged with IBM Content Manager. The event handler toolkit simplifies the creation of custom event handlers for incorporating business logic into versatile solutions that can enhance your existing applications. Two sample programs are also provided as references for the design and implementation of a custom event handler based on the event handler toolkit.

Related information

 [developerWorks: An event-driven framework for integrating IBM Content Manager with IBM FileNet Business Process Manager](#)

[developerWorks: External application integration with IBM Content Manager through a custom event handler](#)

Enabling IBM Content Manager item types to start a FileNet Business Process Manager process with process integration

To enable IBM Content Manager items to start a process, you can create a new item type or modify an existing item type and then define a process integration event subscription for that item type.

Complete the steps to enable IBM Content Manager to connect to the FileNet Business Process Manager workflow process server and retrieve the names of FileNet Business Process Manager process IDs and process attributes. When you configure this connection, you can select FileNet Business Process Manager process IDs and process attributes when you are creating an event subscription in the IBM Content Manager system administration client.

To define process integration event subscriptions, create a new item type or modify an item type and open the Event Subscriptions page. Then, use the following steps to define process integration event subscriptions for item type events that you want the event monitor to track:

1. On the Event Subscriptions page, select **Enable Event Subscriptions**. Then, click **Add**.
2. If the dialog box to log on to the workflow process server opens, enter the user name and password for the workflow process server in the **User name** and **Password** fields.
3. From the **Event type** list, select an event type that you want to start a process.
4. Select **Process integration**.
5. In the **Process ID** field, complete one of the following two actions:

Option	Description
Select a process ID.	If you are logged on to the workflow process server, then select the process ID of a workflow process from the retrieved list.
Type a process ID.	If you are not logged on to the workflow process server, then type the process ID. Ensure that the process ID name is valid because it is not verified by the IBM Content Manager system.

6. To display the system-defined attributes for item types, select **Include system attributes**. By default, only user-defined attributes are displayed in the **Item type attribute** list. Selecting **Include system attributes** includes a subset of IBM Content Manager system-defined attributes in the **Item type attribute** list that you can use for event subscriptions. Examples of system-defined attributes include the user ID of a person who creates or updates a document or the expiration date of a document.
7. From the **Item type attribute** list, select an item type attribute that you want to associate to a process attribute. You can associate a single item type attribute to multiple process attributes. However, for a given event subscription, a process attribute can be associated with a single IBM Content Manager item type attribute only.
8. In the **Process attribute** field, complete one of the following two actions to associate the process attribute with the item type attribute:

Option	Description
Select a process attribute.	If you are logged on to the workflow process server, then select the process attribute from the retrieved list.
Type a process attribute.	If you are not logged on to the workflow process server, then type the process attribute. Ensure that the process attribute name is valid because it is not verified by the IBM Content Manager system.

9. Click **Add** to copy the attribute information to the table of attribute associations.
10. Click **Apply** to save your settings or click **OK** to save your settings and close the window.
11. To make the changes to event subscriptions effective, start the event monitor again.

Related concepts

“Event subscriptions” on page 701

Related tasks

Updating or deleting an event subscription

Starting and stopping the event monitor

Starting and stopping the event handler

Creating an item type

Defining an event subscription for general integration

To enable IBM Content Manager to integrate with applications that are not workflow applications, you can create an item type or modify an existing item type and then define a general integration event subscription for that item type.

To define general integration event subscriptions, create an item type or modify an item type and open the Event Subscriptions page. Then, use the following steps to define general integration event subscriptions for item type events that you want the event monitor to track:

1. On the Event Subscriptions page, select **Enable Event Subscriptions**. Then, click **Add**.
2. If the dialog box to log on to the workflow process server opens, click **Cancel**.
3. From the **Event type** list, select the event type.
4. Select **General integration**.
5. To display the system-defined attributes for item types, select **Include system attributes**. By default, only user-defined attributes are displayed in the **Available attributes** list. Selecting **Include system attributes** includes a subset of IBM Content Manager system-defined attributes in the **Available attributes** list that you can use for event subscriptions. Examples of system-defined attributes include the user ID of a person who creates or updates a document or the expiration date of a document.
6. From the **Available attributes** tree, select an attribute and then click **Add** to add the attribute to the **Selected attributes** list. Repeat this step for all of the attributes that you want to include.
7. Click **Apply** to save your settings or click **OK** to save your settings and close the window.
8. To apply the changes you made to the event subscriptions, start the event monitor again.

Related concepts

“Event subscriptions” on page 701

Related tasks

Updating or deleting an event subscription

Starting and stopping the event monitor

Starting and stopping the event handler

Creating an item type

Updating or deleting an event subscription

If you defined multiple subscriptions for an event type and you want to update or delete a subscription, you must complete some additional maintenance steps.

Important: When you update or delete an event subscription, the system requires 30 seconds for the changes to take effect.

To update or delete a subscription for an event type that is associated with multiple subscriptions:

1. Disable event logging for the item type.
2. Allow the event monitor to process all of the events in the queue.
3. Stop the event monitor and then open the system administration client.
4. Update or delete the event subscriptions.
5. Enable logging for the item type.
6. Close the system administration client and then start the event monitor.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

Portions of this product are:

- Copyright © 2000-2007 The Apache Software Foundation. All Rights Reserved.
- Document Viewer © 1991-2007 MS Technology, Inc. Charlotte, NC. All Rights Reserved.
- Copyright 1994-2007 EMC Corporation. All Rights Reserved
- Copyright ©1998-2003 The OpenSSL Project. All Rights Reserved.
- Oracle® Outside In Viewer Technology, Copyright © 1992, 2007, Oracle. All Rights Reserved.
- Copyright © 1996-1999 by Scott Hudson, Frank Flannery, C. Scott Ananian. All Rights Reserved.
- Copyright 1994-2007 W3C (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University). All Rights Reserved.

This product is Built on Eclipse (<http://www.eclipse.org>).

Trademarks

This topic lists IBM trademarks and certain non-IBM trademarks.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

The following terms are trademarks or registered trademarks of other companies:

Adobe, Acrobat, Portable Document Format (PDF), PostScript, and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Intel, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of IBM or other companies.

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

Glossary

Use the glossary to help you understand terms and abbreviations for IBM Content Manager, IBM Information Integrator for Content, and DB2 Content Manager VideoCharger. Terms shown in *italics* are defined elsewhere in this glossary.

To view glossaries for other IBM products, go to <http://www.ibm.com/software/globalization/terminology/>.

A

abstract class

In object-oriented programming, a class that represents a concept; classes derived from it represent implementations of the concept. An object cannot be constructed from an abstract class; that is, it cannot be instantiated.

access control

The process of ensuring that certain functions and stored *objects* can be accessed only by authorized users in authorized ways.

access control list (ACL)

A list consisting of one or more user IDs or user groups and their associated *privileges*. You use access control lists to control user access to *items* and *objects* in the IBM Content Manager system. You use access control lists to control user access to *search templates* in the system.

accessory script

A CGI *script* that processes SEARCH, POST, PUT, or DELETE requests. The accessory scripts process requests that are not explicitly mapped to a CGI script named on an EXEC directive.

ACL See *access control list*.

action In IBM Content Manager document routing, specifies how a user can manipulate the *work packages* at a *work node*. IBM Content Manager provides some actions and you can create your own. Actions must be included in an *action list* before you can apply them to a work node.

In IBM Information Integrator for Content, specifies how a user can manipulate the *work items* at a *node* in the

workflow. IBM Information Integrator for Content provides some actions and you can create your own. Actions must be included in an *action list* before you can apply them to a *node*.

action list

In IBM Content Manager document routing, a set of *actions* that a user can perform on work packages at a work node. The actions that you specify in the action list are displayed as menu choices for the *work packages* in the client users' *worklists*.

In IBM Information Integrator for Content, a set of *actions* that a user can perform on work items in a *workflow*. The actions that you specify in the action list display as menu choices for the *work items* in the client users' *worklists*.

ad hoc process

In IBM Content Manager document routing, a one step *process* that you define, usually to link two other processes.

address

A unique code or identifier for a register, device, workstation, system, or storage location. See also *IP address*.

administrative ACL

Any *access control list (ACL)* created by an administrator with SystemSetACL and SystemDefineACL *privileges* and to use with administrative objects, such as *item types* and item type views, or *items*. ACLs that you created before Version 8 Release 3 are all administrative ACLs.

admission control

The process used by the server to ensure that the server's bandwidth needs are not compromised by new asset requests.

ADSM

See *Tivoli Storage Manager*.

aggregate bandwidth

Total throughput, in megabits per second, that moves through a server or server subsystem.

alias

In the *Internet*, a name that is assigned to a server that makes the server independent of the name of its host system. The alias must be defined in the *domain name server*.

American Standard Code for Information Interchange (ASCII)

A standard code used for information exchange among data processing systems, data communication systems, and associated equipment. ASCII uses a coded character set consisting of 7-bit coded characters. See also *EBCDIC*.

analog

Pertains to data that consists of continuously variable physical quantities. See also *digital*.

analog video

Video in which the information that represents images is in a continuous-scale electrical signal for amplitude and time.

API

See *application programming interface*.

application programming interface (API)

A software interface that enables applications to communicate with each other. An API is the set of programming language constructs or statements that can be coded in an application program to obtain the specific functions and services provided by the underlying licensed program.

application server

Software that handles communication with the client that requests an asset and queries of IBM Content Manager.

archive

Persistent storage that is used for long-term information retention, typically very inexpensive for each stored unit and slow to access, and often in a different geographic location to protect against equipment failures and natural disasters.

ASCII See *American Standard Code for Information Interchange*.

asset

A digital multimedia resource that is stored for later retrieval as requested by an application. An example of such a

resource is a digitized video or audio file. An asset is stored as a file in a multimedia file system supported by the *data pump*.

asset group

An organizational grouping within the multimedia file system with similar characteristics. You can use an asset group to allocate resources of a *data pump*. For example, you can establish two asset groups representing distinct departments whose assets should be kept separate for security or billing purposes.

asymmetric video compression

In multimedia applications, the use of a powerful computer to compress a video so that a less powerful system can decompress it.

asynchronous transfer mode (ATM)

A transfer mode in which the information is organized into cells; it is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic. ATM is specified in international standards such as ATM Forum UNI 3.1.

ATM

See *asynchronous transfer mode*.

attribute

A unit of data that describes a certain characteristic or property (for example, name, address, age, and so forth) of an item, and which can be used to locate that item. An attribute has a type, which indicates the range of information stored by that attribute, and a value, which is within that range. For example, information about a file in a multimedia file system, such as title, running time, or encoding type (MPEG1, H.263, and so forth). For IBM Information Integrator for Content, see also *federated attribute* and *native attribute*.

attribute group

Convenience grouping of one or more *attributes*. For example, Address might include the attributes Street, City, State, and Zip.

audio

The sound portion of a video signal.

B

background

The conditions under which low-priority, noninteractive programs are run. See also *foreground*.

bandwidth

The difference, expressed in hertz, between the highest and the lowest frequencies of a range of frequencies.

In *asynchronous transfer mode* (ATM), the capacity of a virtual channel, expressed in terms of peak cell rate (PCR), sustainable cell rate (SCR), and maximum burst size (MBS).

A measure of the capacity of a communication transport medium (such as a TV cable) to convey data.

base attributes

A set of indexes that is assigned to each *object*. All IBM Content Manager objects have *base attributes*.

baseband

A frequency band that uses the complete bandwidth of a transmission and requires all stations in the network to participate in every transmission.

batch An accumulation of data to be processed.

A group of records or data processing jobs brought together for processing or transmission.

binary large object (BLOB)

A sequence of bytes with a size ranging from 0 bytes to 2 gigabytes. This string does not have an associated code page and character set. Image, audio, and video objects are stored in BLOBs. See also *character large object* (CLOB).

bitmap

A pixmap with a depth of one bit plane.

A representation of an image by an array of bits.

BLOB See *binary large object*.

block A string of data elements recorded or transmitted as a unit. The elements can be characters, words, or physical records. Disk device drivers currently use a block size of 32 KB or 256 KB to write to the disk.

broadband

A communication channel that uses a wide frequency range divided into narrower bands that can be made available to different users for the simultaneous transmission of different signals (such as voice, video, and data). A broadband is capable of higher-speed data transmission than a voice-grade channel. See also *baseband*.

broadcast

The simultaneous transmission of the same data to all nodes connected to a network. See also *multicast*.

bus A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment.

business application

In IBM Content Manager document routing, a *work node* that directs work to an external business application that you develop. The business application work node has an identified DLL or shared library that runs on the server and can launch an external business application, such as a CICS or IMS program.

C

cache A special-purpose buffer, smaller and faster than main storage, used to hold a copy of data that can be accessed frequently. Use of a cache reduces access time, but might increase memory requirements. See also *resource manager cache* and *LAN cache*.

caching proxy server

A proxy server that stores the documents that it retrieves from other servers in a local *cache*. The caching proxy server can then respond to subsequent requests for these documents without retrieving them from the other servers, a process that can improve response time.

cardinality

The number of rows in a database table.

category

See *item type*.

character large object (CLOB)

A data type that contains a sequence of characters (single-byte, multibyte, or both)

that can range in size from 0 bytes to 2 gigabytes less 1 byte. See also *binary large object*.

child component

Optional second or lower level of a hierarchical *item type*. Each child component is directly associated with the level above it.

CIF See *common interchange file*.

CIU See *common interchange unit*.

class In object-oriented design or programming, a model or template that can be used to create objects with a common definition and common properties, operations, and behavior. An object is an instance of a class.

client A computer system or process that requests a service of another computer system or process that is typically referred to as a server. Multiple clients can share access to a common server.

client application

An application written with the IBM Content Manager APIs to customize a user interface.

An application written with the object-oriented or Internet APIs to access *content servers* from IBM Information Integrator for Content.

Client Application for Windows

A complete object management system that is provided with IBM Content Manager and written with IBM Content Manager APIs. It supports document and folder creation, storage, and presentation, processing, and access control. You can customize the client with user exit routines and partially invoke it with APIs.

client/server

Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

CLOB See *character large object*.

codec A processor that can code analog audio or

video information in digital form for transmission, and decode digital data back to analog form.

collection

A group of objects with a similar set of management rules.

collection event list

In IBM Information Integrator for Content advanced workflow, the criteria that a collection point uses to determine which route the federated folder must follow. Corresponds to a specified amount of time or a list of events, which are *event nodes*. Each collection point must have at least two collection event lists: one with a timeout period (the timeout route) and the other with a list of events that must occur for a federated folder to proceed (event-driven route).

collection point

In IBM Content Manager document routing, a special *work node* at which a folder waits for arrival of other document or folders, but which does not correspond to a business task.

In IBM Information Integrator for Content advanced workflow, a special *node* at which a *federated folder* waits for arrival of other objects, such as documents or folders, or for specified conditions to be met. A collection point consists of one collection node, one to 20 *event nodes*, and two or more connectors called *collection event lists*.

combined search

A query that combines one or more of the following types of searches: *parametric*, text, or image.

common interchange file (CIF)

A file that contains one ImagePlus Interchange Architecture (IPIA) data stream.

common interchange unit (CIU)

The independent unit of transfer for a common interchange file (CIF). It is the part of the CIF that identifies the relationship to the receiving database. A CIF can contain multiple CIUs.

Common Internet File System (CIFS)

A protocol that enables collaboration on the Internet by defining a remote file-access protocol that is compatible with

the way applications already share data on local disks and network file servers.

component

Generic term for a *root component* or a *child component*.

compressed audio

A method of digitally encoding and decoding several seconds of voice quality audio per single videodisc frame. This increases the storage capability to several hours of audio per videodisc. Sometimes referred to as still frame audio or sound over still.

compressed video

A video resulting from the process of digitally encoding and decoding a video image or segment using a variety of computer techniques to reduce the amount of data required to represent the content accurately.

compression

The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks.

connection manager

A IBM Content Manager component that helps maintain connections to the library server, rather than starting a new connection for each query. The connection manager has an application programming interface.

connector class

Object-oriented programming *class* that provides standard access to APIs that are native to specific *content servers*.

constructor method

In programming languages, a method that has the same name as a class and is used to create and initialize objects of that class.

container

A software object that holds or organizes other software objects or entities. In the *folder manager*, an *object* that can contain other folders or documents.

content class

See *MIME type*.

content server

A software system that stores multimedia and business data and the related

metadata required for users to work with that data. IBM Content Manager and ImagePlus for OS/390 are examples of content servers.

controller

The functional component responsible for resource management (load balancing and admission control). The controller communicates with one or more *data pumps* to initiate and terminate connections to clients.

cursor A named control structure used by an application program to point to and select a row of data from a set.

D

data compression

The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks.

data format

A description of the application data for a particular transaction. An application data format is composed of data structures and fields. See also *MIME type*.

data pump

The combination of the disks that hold the data and the networking hardware and software required to deliver assets to clients.

data rate

The rate at which data is transmitted or received from a device. Interactive applications tend to require a high data rate, while batch applications can usually tolerate lower data rates.

data store

A place (such as a database system, file, or directory) where data is stored. In an application program, a virtual representation of a *content server*.

data striping

Storage process in which information is split into blocks (a fixed amount of data) and the blocks are written to (or read from) a series of disks in parallel.

data transfer rate

The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data

transmission system. The rate is expressed in bits, characters, or blocks per second, minute, or hour. Corresponding equipment should be indicated, for example, modems, intermediate equipment, or source and sink.

DCA See *Document Content Architecture*.

DCE See *Distributed Computing Environment*.

DD See *device driver*.

DDO See *dynamic data object*.

decode

To convert data by reversing the effect of some previous encoding.

decompression

Process of restoring compressed data to its original state so that it can be used again.

destager

A function of the *resource manager* that moves objects from the *staging area* to the first step in the object's *migration policy*.

device driver (DD)

A program that provides an interface between a specific device and the application program that uses the device.

device manager

In a IBM Content Manager system, the interface between the *resource manager* and one or more physical devices.

digital Pertaining to data in the form of digits. See also *analog*.

digital audio

Audio tones represented by machine-readable binary numbers rather than by analog recording techniques.

digital video

Video in which the information (usually including audio) is encoded as a sequence of binary digits.

digitize

To convert analog video and audio signals into digital format.

digitized image

An image derived from a scanning device or a digitizing card with a camera.

Distributed Computing Environment (DCE)

The Open Software Foundation (OSF) specification (or a product derived from

this specification) that assists in networking. DCE provides such functions as authentication, directory service (DS), and remote procedure call (RPC).

document

An *item* that can be stored, retrieved, and exchanged among IBM Content Manager systems and users as a separate unit. It can be any multimedia digital object. A single document can include varied types of content, including for example, text, images, and spreadsheets. An item with the document *semantic type* is expected to contain information that forms a document but does not necessarily imply that it is an implementation of the IBM Content Manager document model.

An item created from a document classified item type (a specific implementation of the IBM Content Manager document model), must contain document parts. You can use document classified item types to create items with either the document or folder semantic type. See also *workbasket* and *workflow*.

Document Content Architecture (DCA)

An architecture that guarantees information integrity for a document being interchanged in an office system network. DCA provides the rule for specifying form and meaning of a document. It defines revisable form text (changeable) and final form text (unchangeable).

document root directory

The primary directory in which a Web server stores accessible documents. When the server receives requests that do not point to a specific directory, it tries to serve the requests from this directory.

document routing process

In IBM Content Manager a sequence of *work steps*, and the rules governing those steps, through which a *document* or *folder* travels while it is being processed. See also *work step*.

domain

That part of a computer network in which the data processing resources are under common control.

domain name

In Internet communications, a name of a

host system. A domain name consists of a sequence of subnames that are separated by a delimiter character, for example, *www.ibm.com*.

domain name server

In Internet communications, a server program that supplies name-to-address conversion by mapping domain names to IP addresses.

dotted decimal notation

The syntactical representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 and separated by dots. IP addresses are represented in dotted decimal notation.

dynamic data object (DDO)

In an application program, a generic representation of a stored object that is used to move that object in to, and out of, storage.

dynamic IP address

A temporary IP address for a transient device or logical unit on a network, for example, a personal computer. See also *IP address*.

E

EBCDIC

See *Extended Binary Coded Decimal Interchange Code*.

element

An *object* that the list manager allocates for an application.

encode

To convert data by the use of a code in such a manner that reconversion to the original form is possible.

Ethernet

A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and transmission.

event node

In IBM Information Integrator for Content advanced workflow, the set of criteria that specifies the objects or conditions that are

required by a collection node. Each collection point can include up to 20 event nodes.

Extended Binary Coded Decimal Interchange Code (EBCDIC)

A coded character set of 256 8-bit characters developed for the representation of textual data. See also *American Standard Code for Information Interchange*.

extended data object (XDO)

In an application program, a generic representation of a stored complex multimedia object that is used to move that object in to, and out of, storage. XDOs are most often contained within DDOs.

External Data Representation (XDR)

A standard developed by Sun Microsystems, Incorporated, to represent data in machine-independent format. Because XDR is a vendor-independent method for representing the data, new computer architectures can be integrated into the network without requiring the updating of translation routines.

F

F-Coupler

See *frequency coupler*.

FDDI See *Fiber Distributed Data Interface*.

feature

The visual content information that is stored in the image search server. Also, the visual traits that image search applications use to determine matches. The four *QBIC* features are average color, histogram color, positional color, and texture.

federated attribute

An IBM Information Integrator for Content metadata category that is mapped to *native attributes* in one or more *content servers*. For example, the federated attribute policy number can be mapped to an *attribute policy num* in DB2 Content Manager and to an attribute policy ID in ImagePlus for OS/390.

federated collection

A grouping of objects that results from a federated search. See also *federated search*.

federated data store

Virtual representation of any number of specific content servers, such as IBM Content Manager.

federated entity

An IBM Information Integrator for Content metadata object that is comprised of federated attributes and optionally associated with one or more federated text indexes.

federated folder

In IBM Information Integrator for Content, a special-purpose folder that stores native entities from one or more content servers.

federated search

A query issued from IBM Information Integrator for Content that simultaneously searches for data in one or more content servers, which can be heterogeneous. See also *federated collection*.

federated text index

An IBM Information Integrator for Content metadata object that is mapped to one or more *native text indexes* in one or more *content servers*.

Fiber Distributed Data Interface (FDDI)

An American National Standards Institute (ANSI) standard for a 100-Mbps LAN using fiber optic cables.

file name extension

An addition to a file name that identifies the file type (for example, text file or program file).

file system

The collection of files and file management structures on a physical or logical mass storage device, such as a diskette or minidisk.

file system manager

The component that manages the multimedia file system.

File Transfer Protocol (FTP)

In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

firewall

A network configuration, usually both

hardware and software, that prevents unauthorized traffic into and out of a secure network.

folder An *item* of any *item type*, regardless of classification, with the folder *semantic type*. Any item with the folder semantic type contains specific folder functionality that is provided by IBM Content Manager, in addition to all non-resource item capabilities and any additional functionality available from an item type classification, such as *document* or resource item. Folders can contain any number of items of any type, including documents and subfolders. A folder is indexed by *attributes*.

folder manager

The IBM Content Manager model for managing data as online documents and folders. You can use the folder manager APIs as the primary interface between your applications and the IBM Content Manager content servers.

foreground

In multiprogramming, the environment in which high-priority programs are run. See also *background*.

FPS See *frames per second*.

fragment

The smallest unit of file system disk space allocation. A fragment can be 512, 1024, 2048, or 4096 bytes in size. The fragment size is defined when a file system is created.

frames per second (FPS)

The number of frames displayed per second.

frequency coupler (F-Coupler)

A physical device that merges broadband analog signals with digital data on an IBM Cabling System using shielded twisted-pair wiring. The IBM F-Coupler separates analog signals and sends them from the IBM Cabling System to the workstation. The F-Coupler allows the IBM Cabling System to accommodate simultaneous analog video with data traffic on a token-ring network.

FTP See *File Transfer Protocol*.

full-motion video

Video reproduction at 30 frames per second (*fps*) for *NTSC* signals or 25 *fps* for *PAL* signals.

G**gateway**

A device or program used to connect networks or systems with different network architectures.

GB See *gigabyte*.

Gbps See *gigabits per second*.

gigabits per second (Gbps)

A measure of high speed bandwidth on a digital data transmission medium such as optical fiber. See also *kilobits per second*.

gigabyte (GB)

In decimal notation, 1 073 741 824 when referring to memory capacity; in all other cases, it is defined as 1 000 000 000.

H**handle**

A character string that represents an object and is used to retrieve the object.

hertz (Hz)

A unit of frequency equal to one cycle per second.

history log

A file that keeps a record of activities for a *workflow*.

home page

The initial Web page that is returned by a Web site when a user specifies the URL for the Web site. Essentially, the home page is the entry point for accessing the contents of the Web site.

host

A computer that is connected to a network and provides an access point to that network. The host can be a client, a server, or both a client and server simultaneously. See also *server*, *client*.

host name

In *Internet* communication, the name given to a computer. Sometimes, host name is used to mean the fully qualified domain name; other times, it is used to mean the most specific subname of a fully qualified domain name. For example, if *mycomputer.city.company.com* is the fully

qualified domain name, either of the following host names can be used: *mycomputer.city.company.com* or *mycomputer*.

HTML

See *Hypertext Markup Language*.

HTTP See *Hypertext Transfer Protocol*.

HTTPd

See *HTTP daemon*.

HTTP daemon (HTTPd)

A multithreaded Web server that receives incoming *Hypertext Transfer Protocol* (*HTTP*) requests.

HTTP method

An action that is used by the *Hypertext Transfer Protocol*. *HTTP* methods include GET, POST, and PUT.

Hypertext Markup Language (HTML)

A markup language that conforms to the Standard Generalized Markup Language (SGML) standard and was designed primarily to support the online display of textual and graphical information, including hypertext links.

Hypertext Transfer Protocol (HTTP)

An Internet protocol that is used to transfer and display hypertext and XML documents on the Web.

Hz See *hertz*.

I**I frame**

See *information frame*.

Image Object Content Architecture (IOCA)

An architecture that provides a collection of constructs used to interchange and present images, such as printing image data on a page, page segment, or overlay.

index To add or edit the attribute values that identify a specific *item* or *object* so that it can be retrieved later.

index class

See *item type*.

index class subset

In earlier IBM Content Manager, a view of an *index class* that an application uses to store, retrieve, and display folders and objects.

index class view

In earlier IBM Content Manager, a term used in the APIs for *index class subset*.

information frame (I frame)

In video compression, a frame that is compressed independently of any other frames.

information mining

The automated process of extracting key information from text (summarization), finding predominant themes in a collection of documents (categorization), and searching for relevant documents using powerful and flexible queries.

inline In IBM Content Manager, the property of an object that is online and in a drive but has no active *mounts*.

i-node The internal structure that describes the individual files in the UNIX file system. An i-node contains the node, type, owner, and location of a file. A table of i-nodes is stored near the beginning of a *file system*.

interactive video

Combining video and computer technology so the user's actions determine the sequence and direction the application takes.

interchange

To import or export an image with its index from one IBM Content Manager ImagePlus for OS/390 system to another ImagePlus system using a *common interchange file* or *common interchange unit*.

Internet

The worldwide collection of interconnected networks that use the Internet suite of protocols and permit public access.

Internet Protocol (IP)

A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also *Transmission Control Protocol*.

Internet Protocol address

See *IP address*.

intra frame

See *information frame*.

intranet

An organization's internal network that uses the IP protocol.

IOCA See *Image Object Content Architecture*.

IP See *Internet Protocol*.

IP address (Internet Protocol address)

A unique address for a device or logical unit on a network that uses the IP standard. See also *static IP address*, *dynamic IP address*.

IP multicast

Transmission of an *Internet Protocol (IP)* datagram to a set of systems that form a single multicast group.

ISO-9669

Format used for files on CD-ROM. Used with DOS.

isochronous

Property of a communications signal that is delivered at a specified, bounded rate, which is used for continuous data such as voice and full-motion video.

item In IBM Content Manager, generic term for an instance of an *item type*. For example, an item might be a *folder*, *document*, video, or image. See also *semantic type*.

Generic term for the smallest unit of information that IBM Information Integrator for Content administers. Each item has an identifier. For example, an item might be a *folder* or a *document*.

item type

A template for defining and later locating like items, consisting of a *root component*, zero or more *child components*, and a classification. See also *item type classification*.

item type classification

A categorization within an *item type* that further identifies the items of that item type. All items of the same item type have the same item type classification. See also *index class*.

IBM Content Manager, supplies the following item type classifications: *folder*, *document*, *object*, video, image, and text; users can also define their own item type classifications.

iterator

A class or construct that is used to step through a collection of objects one at a time.

K

Kb See *kilobit*.

kbps See *kilobits per second*.

key field

See *attribute*.

kilobit (Kb)

For processor storage, real and virtual storage, and channel volume, 2 to the power of 10 or 1024 bits.

For disk storage capacity and communications volume, 1000 bits.

kilobits per second (kbps)

A measure of bandwidth on a data transmission medium, where 1 kb/s = 1000 bits per second. This contrasts with units of storage where 1 Kb = 1024 bits (note uppercase K). See also *megabits per second*, *gigabits per second*.

L

latency

The time interval between the instant at which an instruction control unit initiates a call for data and the instant at which the actual transfer of the data starts.

LBR See *low bit rate*.

library client

The component of a IBM Content Manager system that provides a low-level programming interface for the library system. The library client includes APIs that are part of the software developer's kit.

library object

See *item*.

library server

The component of a IBM Content Manager system that stores, manages, and handles queries on *items*.

link

A directional relationship between two items: the parent and the child. You can use a set of links to model one-to-many associations. See also *reference*.

log record sequence number (LRSN)

A unique identifier for a log record that is associated with a data sharing member. DB2 for z/OS uses the LRSN for recovery in the data sharing environment.

low bit rate (LBR)

A generic term for an interleaved H.263/G.723 stream. Low bit rate streams range from 6.4 kbps up to 384 kbps.

LRSN See *log record sequence number*.

M

machine-generated data structure (MGDS)

An IBM structured data format protocol for passing character data among the various IBM Content Manager ImagePlus for OS/390 programs.

Data extracted from an image and put into general data stream (GDS) format.

management class

The term used in the APIs for *migration policy*.

Management Information Base (MIB)

A collection of objects that can be accessed by means of a network management *protocol*.

Management Information Base variable (MIB variable)

A managed object that contains pertinent management information, which is accessible as defined by the access mode. The MIB variable is defined by a textual name and the corresponding object identifier, syntax, access mode, and status, and a description of the semantics of the managed object.

maximum transmission unit (MTU)

The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the maximum transmission unit for Ethernet is 1500 bytes.

Mb See *megabit*.

MB See *megabyte*.

Mbps See *megabits per second*.

MCA See *Micro Channel architecture*.

media archiver

A physical device that is used for storing audio and video stream data. The

VideoCharger is a type of media archiver.
See also *storage system*.

media object class

Classification that describes the data that is contained in an object and how you can act on that data. IBM Content Manager provides four predefined media object classes: DKLobICM, DKStreamICM, DKTextICM, and DKVideoStreamICM. See also *MIME type*.

media server

An AIX-based component of the IBM Content Manager system that is used for storing and accessing video files.

megabit (Mb)

For processor storage, real and virtual storage, and channel volume, 2 to the power of 20 or 1 048 576 bits. For disk storage capacity and communications volume, 1 000 000 bits.

megabits per second (Mbps)

See *kilobits per second*.

megabyte (MB)

For processor storage, real and virtual storage, and channel volume, 2 to the 20th power or 1 048 576 bytes. For disk storage capacity and communications volume, 1 000 000 bytes.

member function

A C++ operator or function that is declared as a member of a class. A member function has access to the private and protected data members and member functions of an object of its class. Member functions are also called methods.

method

In object-oriented design or programming, the software that implements the behavior specified by an operation.

See *member function*.

MGDS

See *machine-generated data structure*.

MIB See *Management Information Base*.

MIB variable

See *Management Information Base variable*.

Micro Channel architecture (MCA)

The rules that define how subsystems and adapters use the Micro Channel bus in a computer. MCA defines the services that each subsystem can or must provide.

MIDI See *Musical Instrument Digital Interface*.

migration

The process of moving data and source from one computer system to another computer system without converting the data, such as when moving to a new operating environment.

Installation of a new version or release of a program to replace an earlier version or release.

migration policy

A user-defined schedule for moving *objects* from one *storage class* to the next. It describes the retention and class transition characteristics for a group of objects in a storage hierarchy.

migrator

A function of the *resource manager* that checks *migration policies* and moves objects to the next storage class when they are scheduled to move.

Mixed Object Document Content Architecture (MO:DCA)

An IBM-architected, device-independent data stream for interchanging documents.

Mixed Object Document Content Architecture-Presentation (MO:DCA-P)

A subset of MO:DCA that defines presentation documents.

M-JPEG

See *Motion JPEG*.

MO:DCA

See *Mixed Object Document Content Architecture*.

MO:DCA-P

See *Mixed Object Document Content Architecture-Presentation*.

Motion JPEG (M-JPEG)

Used for animation.

mounted

In IBM Content Manager, an object that is online and in a drive with active *mounts*. Contrast with *inline*.

Moving Pictures Experts Group (MPEG)

A group that is working to establish a standard for compressing and storing motion video and animation in digital form.

The standard developed by the Moving Pictures Experts Group.

MPEG

See *Moving Pictures Experts Group*.

MTU See *maximum transmission unit*.

multicast

Transmission of the same data to a selected group of destinations. See also *broadcast* and *unicast*.

multimedia

Material presented in a combination of text, graphics, video, animation, and sound.

multimedia file system

A *file system* that is optimized for the storage and delivery of video and audio.

Multipurpose Internet Mail Extensions (MIME)

An Internet standard for identifying the type of object being transferred across the Internet. See also *MIME type*.

Musical Instrument Digital Interface (MIDI)

A *protocol* that allows a synthesizer to send signals to another synthesizer or to a computer, or a computer to a musical instrument, or a computer to another computer.

N

NAS See *network attached storage*.

National Television Standard Committee (NTSC)

A committee that sets the standard for color television broadcasting and video in the United States (currently in use also in Japan).

native attribute

A characteristic of an object that is managed on a specific *content server* and that is specific to that content server. For example, the *key field* policy num might be a native attribute in an IBM Content Manager content server whereas the field policy ID might be a native attribute in a Content Manager OnDemand content server.

native entity

An *object* that is managed on a specific *content server* and that is comprised of *native attributes*. For example, IBM

Content Manager index classes are native entities comprised of IBM Content Manager key fields.

native text index

An index of the text *items* that are managed on a specific *content server*. For example, a single text search index on an IBM Content Manager content server.

network attached storage (NAS)

A technology in which an integrated storage system is attached to a messaging network that uses common communications protocols, such as *TCP/IP*.

network table file

A text file that contains the system-specific configuration information for each node in an IBM Content Manager system. Each node in the system must have a network table file that identifies the node and lists the nodes that it needs to connect to. The name of a network table is FRNOLINT.TBL.

node In networking, a point capable of sending and receiving data. A node can be a device, such as printer or workstation, a system, or a storage location on a disk. See also *port*.

In IBM Information Integrator for Content advanced workflow, a generic term for any discrete point in a workflow process.

NTSC See *National Television Standard Committee*.

O

object Any digital content that a user can manipulate as a single unit to perform a task. An object can appear as text, an icon, or both.

object server

See *resource manager*.

object server cache

See *resource manager cache*.

overlay

A collection of predefined data, such as lines, shading, text, boxes, or logos, that can be merged with variable data on a page or form while printing.

P

package

A collection of related *classes* and interfaces that provides access protection and namespace management.

page pool

The area in the shared memory segment from which buffers are allocated for data that is read from or written to disk. Page pool size is one of the file manager startup configuration parameters.

PAL See *phase alternation line*.

parametric search

A query for *objects* that is based on the *properties* of the objects.

part See *object*.

patron The term used in the IBM Content Manager APIs for *user*.

pattern-matching character

See *wildcard character*.

PCI See *Peripheral Component Interconnect*.

peak rate

The maximum rate encountered over a given period of time.

performance group

A group of file systems sharing system resources that can affect file system performance.

Peripheral Component Interconnect (PCI)

A local bus that provides a high-speed data path between the processor and attached devices.

persistent identifier (PID)

An identifier that uniquely identifies an object, regardless of where it is stored. The PID consists of both an item ID and a location.

phase alternation line (PAL)

The television broadcast standard for European video outside of France and the countries of the former Soviet Union. See also *National Television Standard Committee*.

physical data block

A string of data elements or a group of records that is received, recorded, processed, or transmitted as a unit.

PID See *persistent identifier*.

port An access point, for example, a logical unit, for data entry or exit. See also *node*.

In the Internet suite of protocols, a specific logical connection between the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) and a higher level protocol or application.

port group

A logical name used to group one or more ports (network devices or interfaces) of the same network type that can be used to reach a given end-user destination. For example, if multiple ATM adapters in the IBM DB2 Content Manager VideoCharger Server complex are connected to the same ATM networks, these adapters can be configured under the same port group. The controller selects ports as necessary to balance the load.

presentation formatter

A CGI program that defines the forms used to select and present assets to clients.

privilege

The right to access a specific database *object* in a specific way. Privileges are controlled by users with SYSADM (system administrator) authority or DBADM (database administrator) authority or by creators of objects. For example, privileges can include rights to create, delete, and retrieve data from tables.

privilege set

A collection of *privileges* for working with system components and functions. The administrator assigns privilege sets to users (user IDs) and *user groups*.

process

In IBM Content Manager document routing, a series of steps through which work is routed. A process contains at least one start node, one *work node*, and one stop node.

property

A characteristic of an *object* that describes the object. A property can be changed or modified. Properties can describe an object's name, type, value, or behavior, among other things.

protocol

A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

protocol gateway

A type of *firewall* that protects computers in a business network from access by users outside that network.

proxy server

A server that receives requests intended for another server and that acts on the client's behalf (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

purger

A function of the *resource manager* that removes *objects* from the system.

Q

QBIC See *Query by Image Content*.

QoS See *quality of service*.

quality of service (QoS)

For an *asynchronous transfer mode (ATM)* virtual channel or a Networking BroadBand Services (NBBS) network connection, a set of communication characteristics such as end-to-end delay, jitter, and packet loss ratio.

Query by Image Content (QBIC)

A query technology that enables searches based on visual content, called features, rather than plain text. Using QBIC, you can search for objects based on their visual characteristics, such as color and texture.

query string

A character string that specifies the properties and property values for a query. You can create the query string in an application and pass it to the query.

R

RAID See *Redundant Array of Independent Disks*.

rank An integer value that signifies the

relevance of a given part to the results of a query. A higher rank signifies a closer match.

real time

The processing of information that returns a result so rapidly that the interaction appears to be instantaneous.

Real-Time Transport Protocol (RTP)

A *protocol* that provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services.

rebalance

To restripe and redistribute data across the available hard disks after a disk or disks have been removed from a *file system*.

Redundant Array of Independent Disks (RAID)

A collection of two or more physical disk drives that present to the host an image of one or more logical disk drives. In the event of a single device failure, the data can be read or regenerated from the other disk drives in the array.

reference

Single direction, one-to-one association between a root or *child component* and another *root component*. See also *link*.

reference frame

See *information frame*.

release

To remove suspend criteria from an *item*. A suspended item is released when the criteria have been met, or when a user with proper authority overrides the criteria and manually releases it.

Remote Method Invocation (RMI)

A set of APIs that enables distributed programming. An object in one Java Virtual Machine (JVM) can invoke methods on objects in other JVMs

Remote Procedure Call (RPC)

A protocol that allows a program on a client computer to run a program on a server.

render To take data that is not typically image-oriented and depict or display it as an image. In IBM Content Manager,

word-processing documents can be rendered as images for display purposes.

request

The part of a Web address that follows the *protocol* and server *host name*. For example, in the address `http://www.server.com/rfoul/sched.htm`, the request is `/rfoul/sched.html`.

ReSerVation Protocol (RSVP)

A resource reservation setup *protocol* designed for an integrated services Internet. The protocol provides receiver-initiated setup of resource reservations for multicast and unicast data flows.

resource manager

The component of an IBM Content Manager system that manages *objects*. These objects are referred to by *items* stored on the *library server*.

resource manager cache

The working storage area for the *resource manager*.

restripping

Redistributing and rebalancing data across all available and defined disks in a multimedia file system. This is typically done when a disk is removed from a file system for repair or when a new disk is added to a *file system*.

RLE See *run-length encoding*.

RMI See *Remote Method Invocation*.

RMI server

A server that implements the Java Remote Method Invocation (RMI) distributed object model.

root component

The first or only level of a hierarchical *item type*, consisting of related system-defined and user-defined *attributes*.

RPC See *Remote Procedure Call*.

RSVP See *ReSerVation Protocol*.

RTP See *Real-Time Transport Protocol*.

run A string of repeated, adjacent characters or symbols. See also *run-length encoding*.

run-length encoding (RLE)

A type of *compression* that is based on

strings of repeated, adjacent characters or symbols, which are called *runs*. See also *run*.

S

SCSI See *Small Computer System Interface*.

search criteria

Attribute values that are used to retrieve a stored *item*.

In IBM Information Integrator for Content, specific fields that an administrator defines for a search template that limit or further define choices available to the users.

search template

A form consisting of search criteria designed by an administrator for a specific type of federated search. The administrator also identifies the *users* and *user groups* who can access each search template.

semantic type

The usage or rules for an item. Base, annotation, and note are semantic types supplied by IBM Content Manager. Users can also define their own semantic types. See also *item*.

server A software program or a computer that provides services to other software programs or other computers. See also *host* and *client*.

server definition

The characteristics of a specific *content server* that uniquely identify it to IBM Information Integrator for Content.

server inventory

The comprehensive list of *native entities* and *native attributes* from specified *content servers*.

server type definition

The list of characteristics, as identified by the administrator, required to uniquely identify a custom server of a certain type to IBM Information Integrator for Content.

Simple Network Management Protocol (SNMP)

A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a *Management Information Base (MIB)*.

Small Computer System Interface (SCSI)

A standard hardware interface that enables a variety of peripheral devices to communicate with one another.

SMIT See *System Management Interface Tool*.

SMS See *system-managed storage*.

SNMP

See *Simple Network Management Protocol*.

staging

The process of moving a stored *object* from an offline or low-priority device to an online or higher priority device, usually on demand of the system or on request of the user. When a user requests an object stored in permanent storage, a working copy is written to the *staging area*.

staging area

The working storage area for the *resource manager*. Also referred to as *resource manager cache*.

stand-alone system

A preconfigured IBM Content Manager system that installs all of the components of an IBM Content Manager system on a single personal computer.

static IP address

A fixed IP address for a persistent device or logical unit on a network that uses the IP standard. See also *IP address*.

sticky pool

The part of the page pool that is made available to cache the first block of frequently used interactive files. Sticky pool size is one of the file manager startup configuration parameters.

still frame

See *information frame*.

storage class

The type of media that an object is stored on. It is not directly associated with a physical location. However, it is directly associated with the *device manager*. Types of storage classes include:

- Fixed disk
- VideoCharger
- Media archive
- Tivoli Storage Manager (including optical, stream, and tape)

See also *storage group*, *storage system*.

storage group

A group that associates a storage system to a storage class. See also *storage class* and *storage system*.

storage system

A generic term for storage in the IBM Content Manager system. See also *media archiver*, *storage class*, and *storage group*.

streamed data

Any data sent over a network connection at a specified rate. A stream can be one data type or a combination of types. Data rates, which are expressed in bits per second, vary for different types of streams and networks.

stripe group

A collection of disks that are grouped together for serving media streams. The multimedia file system uses stripe groups to optimize delivery of multimedia *assets*.

stripe width

The size of the block that data is split into for *striping*.

striping

Splitting data to be written into equal blocks and writing blocks simultaneously to separate disk drives. Striping maximizes performance to the disks. Reading the data back is also scheduled in parallel, with a block being read concurrently from each disk then reassembled at the host..

subclass

A *class* that is derived from another class. One or more classes might be between the class and subclass.

subprocess

In IBM Content Manager document routing, an existing process that you define to run within another process.

sub-workflow

In IBM Information Integrator for Content advanced workflow, an existing workflow process that is checked in to the workflow server that you define to run within another workflow.

superclass

A *class* from which a class is derived. One or more classes might be between the class and superclass.

suspend

To remove an *object* from its *workflow* and define the suspension criteria needed to activate it. Later activating the object enables it to continue processing.

system-managed storage (SMS)

Storage managed by the storage management subsystem (SMS). The system determines object placement, and automatically manages object backup, movement, space, and security.

System Management Interface Tool (SMIT)

An interface tool of the AIX operating system for installing, maintaining, configuring, and diagnosing tasks.

T

table of contents (TOC)

The list of *documents* and *folders* that are contained in a folder or *workbasket*. Search results are displayed as a folder table of contents.

Tagged Image File Format (TIFF)

A file format for storing high-quality graphics.

throughput

A measure of the amount of information transmitted over a network in a given period of time. It is generally measured in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps). See also *aggregate bandwidth*.

TIFF See *Tagged Image File Format*.

Tivoli Storage Manager

A *client/server* product that provides storage management and data access services in a heterogeneous environment. Tivoli Storage Manager supports various communication methods, provides administrative facilities to manage the backup and storage of files, and provides facilities for scheduling backups.

token ring

According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations.

token-ring network (TRLAN)

A local area network that connects devices in a ring topology and allows unidirectional data transmission between

devices by a token-passing procedure. A device must receive a token before it can transmit data.

topology

The physical or logical mapping of the location of networking components or nodes within a network. Common network topologies include bus, ring, star, and tree.

TRLAN

See *token-ring network*.

TSM See *Tivoli Storage Manager*.

TSM volume

A logical area of storage that is managed by *Tivoli Storage Manager*.

U

UDP See *User Datagram Protocol*.

unicast

Transmission of data to a single destination. See also *multicast*.

user For IBM Content Manager, this term generally refers to users of client applications, rather than the developers of applications, who use the IBM Content Manager APIs.

In IBM Information Integrator for Content, anyone who is identified in the IBM Information Integrator for Content administration program.

user ACL

Any *access control list (ACL)* created by an end *user* with *UserACLOwner privilege* and can be assigned only to *items*. Users can search on user ACLs. User ACLs are not displayed in the system administration client. A user who is listed in the user ACL and who has *UserACLOwner privilege*, or an administrator, can modify a user ACL by using the APIs.

User Datagram Protocol (UDP)

An *Internet* protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process.

user exit

A point in a program at which a user exit routine may be given control.

user exit routine

A user-written routine that receives control at predefined *user exit* points.

user group

A group consisting of one or more defined individual *users*, identified by a single group name.

user mapping

The association of IBM Information Integrator for Content user IDs and passwords to corresponding user IDs and passwords in one or more content servers. User mapping enables single logon to IBM Information Integrator for Content and multiple *content servers*.

utility server

An IBM Content Manager component that is used by the database utilities for scheduling purposes. You configure a utility server when you configure a *resource manager* or *library server*. There is one utility server for each resource manager and each library server.

V**video mixing**

The process of dynamically inserting or combining multiple *video objects* into a single object for distribution. An example would be the mixing of commercials and broadcast programs for satellite distribution.

video object

The data file containing a program recorded for playback on a computer or television set.

video-on-demand (VOD)

A service for providing consumers with movies and other programming almost immediately, per request.

video stream

The path data follows when read from the DB2 Content Manager VideoCharger Server system to the display unit.

virtual node

In IBM Content Manager document routing, a distinguishable point within your *process* diagram at which no work is

performed or decisions made, but which is required to effectively render the process flow. Start, stop, split, and join are virtual nodes.

VOD See *video-on-demand*.

volume

A representation of an actual physical storage device or unit on which the objects in your system are stored.

W

WAIS See *Wide Area Information Service*.

WAV A format to store digitally recorded sound.

Web server

A server that is connected to the *Internet* and is dedicated to serving Web pages.

Wide Area Information Service (WAIS)

A network information system that enables clients to search documents on the World Wide Web.

workbasket

In IBM Content Manager document routing, a location at which work waits for action by a user or an application. The action can either be taken on the work waiting at the work basket, or the action can be routing the work to another *work node*.

In Content Manager Version 7 workflow, synonymous with *worklist*.

workflow

In IBM Information Integrator for Content, a sequence of work steps, and the rules governing those steps, through which work is routed. For example, claims approval would describe the process that an individual insurance claim must follow for approval. See also *document*, *work packet*, and *work step*.

workflow coordinator

In earlier IBM Content Manager workflow, a user who receives notification that a *work item* in the *workflow* has not been processed in some specified time. The user is selected for a specific user group or upon creation of the workflow.

workflow state

The status of an entire *workflow*.

work item

In earlier IBM Content Manager workflow and IBM Information Integrator for Content advanced workflow, a document or object that a user requires to complete a *workflow* activity.

work node

In IBM Content Manager document routing, a step within a process at which items wait for actions to be completed by end users or applications, or through which items move automatically. Generic term for one of the following three types of work nodes: work basket, collection point, and business application.

In IBM Information Integrator for Content advanced *workflow*, a step within a workflow where work is performed by specified users or groups.

worklist

A collection of work items, documents, or folders that are assigned to a user or group.

work package

In IBM Content Manager document routing, a system-defined object that references the item that a user works on during a process. In addition to the item ID, the work package contains additional information that identifies the process to which it belongs and its priority, state, and resume time (if suspended). The user is unaware of a work package because the user works on the referenced item, not on the work package itself.

work packet

In Enterprise Information Portal Version 7.1, a collection of *documents* that is routed from one location to another. Users access and work with work packets through *worklists*. See also *workflow*.

work state

The status of an individual work item, document, or folder.

work step

A discrete point in a workflow or document routing process through which an individual work item, document, or folder must pass. See also *document routing process* and *workflow*.

X

XDO See *extended data object*.

XDR See *External Data Representation*.

Index

A

- access control lists
 - assigning privilege sets to 513
 - binding level 472
 - changing the ACL optimization modes 25
 - copying 475
 - creating 471
 - defining 472
 - deleting user ACL 474
 - description 472
 - designing for document routing
 - example 268
 - sample procedure 265
 - designing for workflow (IBM Information Integrator for Content), sample procedure 531
 - evaluating ACL optimization modes 27
 - modifying 473
 - moving between domains 522
 - predefined 472
 - testing ACL optimization modes 29
 - troubleshooting 659
 - viewing 473
 - access types
 - adding 53
 - deleting 48
 - description 53
 - modifying 53
 - viewing 53
 - accessibility
 - display features 3
 - documentation 3
 - features that provide 1
 - graphical process builder 303
 - keyboard 1
 - keyboard shortcuts 2
 - screen readers, compatible 3
 - ACL optimization modes
 - changing 25
 - evaluating 27
 - testing performance 29
 - action lists
 - document routing
 - copying 275
 - creating 274
 - description 274
 - modifying 274
 - viewing 274
 - IBM Information Integrator for Content workflow
 - copying 537
 - creating 535
 - description 536
 - modifying 536
 - viewing 536
 - actions
 - document routing
 - copying 272
 - creating 269
 - actions (*continued*)
 - document routing (*continued*)
 - description 270
 - modifying 271
 - viewing 271
 - IBM Information Integrator for Content workflow
 - copying 534
 - creating 532
 - description 533
 - modifying 534
 - viewing 534
 - ad hoc routing, description 305
 - administration
 - changing passwords 662
 - IBM Content Manager , overview 103
 - IBM Information Integrator for Content, overview 105
 - administration authority 429
 - administration client
 - cataloging the DB2 node and database on UNIX and Windows 73
 - manually connecting to DB2
 - administration database 73
 - cataloging the DB2 node and database on z/OS 73
 - cataloging variables 74
 - DB2 Configuration Assistant 72
 - messages 579
 - troubleshooting 579
 - administration database
 - connecting the system administration client 67
 - locating connection information 68
 - manually connecting the
 - administration client
 - cataloging the DB2 node and database on UNIX and Windows 73
 - cataloging the DB2 node and database on z/OS 73
 - connecting to a DB2 administration database 72
 - database cataloging variables 74
 - DB2 Configuration Assistant 72
 - password reference 662
 - server configuration utility 70
- administrative domains
 - assigning a collection to 520
 - assigning user group to 520
 - copying 519
 - creating 517
 - defining replication rules 366
 - deleting 519
 - description 517
 - enabling 516
 - modifying 518
 - subadministrator privileges 517
 - superadministrator privileges 517
 - viewing 518

- AllowConnectToLogon privilege 478
- AllowTrustedLogon privilege 478
- API logs
 - cmblogconfig.properties 653
 - dklog.log 653
- AS/400 server 38
- attribute groups
 - copying 152
 - creating 151
 - deleting 152
 - description 149, 151
 - modifying 151
 - viewing 151
- attributes
 - copying 150
 - creating 146
 - deleting 150
 - description 149
 - mapping 81
 - modifying 150
 - multi-valued 165
 - tips for non-English use 594
 - viewing 150
- authentication
 - of users 429
- authentication failure 599
- auto-folding 188
- auto-linking
 - definition 188
 - example 142
- automatic workflow, establishing for document routing 317

B

- backups
 - pausing processing before 368
 - resuming processing after 369
- BPM, see FileNet Business Process Manager 683
- branches, IBM Information Integrator for Content
 - collection event list 555
 - exit condition 556
- builder, document routing
 - launching 294
 - tools 301
- business applications (document routing)
 - adding to a process 304
 - copying 293
 - defining 291
 - deleting 294
 - description 292
 - modifying 293
 - viewing 293

C

- cardinality 165
- CCSID 202, 209

- ChangeSMS 649
 - characters
 - 7-bit ASCII 578
 - child components
 - cardinality 165
 - cascade delete rule 165
 - defining 165
 - example 165
 - restrict delete rule 165
 - client
 - document item types 142
 - support for data model elements 128
 - Client for Windows
 - action list, description 274
 - action, creating 269
 - ad hoc routing 305
 - connectors display in 306
 - defining item types for use with 160
 - notification flag 295
 - worklist
 - description 314
 - planning 260
 - client, system administration
 - description 106
 - First Steps introduces
 - IBM Content Manager 104
 - ClientAddNewBasePart privilege 478
 - ClientAddToNoteLog privilege 478
 - ClientAdvancedSearch privilege 478
 - ClientDeleteBasePart privilege 478
 - ClientExport privilege 478
 - ClientGetWorkList privilege 478
 - ClientImport privilege 478
 - ClientModifyAnnotation privilege 478
 - ClientModifyBasePart privilege 478
 - ClientModifyNoteLog privilege 478
 - ClientPrint privilege 478
 - ClientReadAnnotation privilege 478
 - ClientReadBasePart privilege 478
 - ClientReadHistory privilege 478
 - ClientReadNoteLog privilege 478
 - ClientScan privilege 478
 - ClientUserAllPrivs privilege set 509
 - ClientUserCreateandDelete privilege set 509
 - ClientUserEdit privilege set 509
 - ClientUserReadOnly privilege set 509
 - cmbcc2mime.ini 100
 - cmbds.ini
 - locating 585
 - parameters 75
 - cmbemconfig.properties 599, 600
 - cmbicmsrvs.ini
 - locating 585
 - parameters 75
 - troubleshooting 602
 - CMBROOT 571
 - collection event lists (IBM Information Integrator for Content workflow)
 - creating 555
 - description 556
 - collection nodes (IBM Information Integrator for Content workflow),
 - creating 553
 - collection points
 - document routing
 - adding to a process 304
 - collection points (*continued*)
 - document routing (*continued*)
 - copying 289
 - creating 283
 - deleting 294
 - description 285
 - modifying 286
 - viewing 286
 - IBM Information Integrator for Content workflow
 - creating 553
 - description 553
 - collection type
 - changing 170, 171
 - collections
 - assigning to a domain 520
 - assigning users to 464
 - copying 361
 - creating 356
 - deleting 362
 - description 360
 - modifying 361
 - moving domains 522
 - OAM 357
 - Tivoli Storage Manager on z/OS 358
 - viewing 361
 - commands
 - cmbwfstart, for starting MQ Workflow server 528
 - EIPUser2WF.bat
 - for adding users to MQ Workflow server 530
 - for deleting users from MQ Workflow server 530
 - common log directory 398
 - common time stamp 398
 - components
 - child 165
 - defining default table spaces 167, 168
 - overview 164
 - root 165
 - configuration
 - with FileNet Business Process Manager 686
 - configuration profiles
 - library server 5
 - resource manager 56
 - configuring
 - resource manager log files 405
 - connecting 38
 - connection and configuration strings,
 - defining 34
 - connection port
 - identifying on UNIX 69
 - identifying on Windows 69
 - identifying on z/OS 69
 - connectors
 - document routing process,
 - creating 306
 - IBM Information Integrator for Content
 - collection event lists 555
 - exit condition 556
 - overview 33
 - content class 193
 - content encryption
 - server definition 64
 - Content Manager for AS/400 server 38
 - Content Manager for z/OS high-volume batch load utility
 - supported functions 238
 - usage guidelines 238
 - Content Manager for z/OS high-volume batch update utility
 - supported functions 240
 - usage guidelines 240
 - Content Manager OnDemand server
 - defining 36
 - content server definition
 - copying 39
 - modifying 38
 - overview 32
 - viewing 38
 - conventions 108
 - criteria settings
 - defining
 - manually 96
 - with the wizard 93
 - CTE0143 error 610
 - cycles, setting 57
- ## D
- data
 - backing up 368
 - exporting as XML 218
 - importing from an XML file 221
 - preparing to back up 368
 - restoring 368
 - data access, managing 470
 - data model scenarios
 - modeling insurance data 139
 - modeling journal article data 139
 - modeling your data 137
 - data modeling
 - attribute groups 151
 - attributes 146
 - custom data model 136
 - database indexes 198
 - foreign keys 178
 - introduction 123
 - item type subsets 200
 - item types 156
 - link types 174
 - media object (XDO) classes 195
 - MIME types 192
 - options 190
 - planning 125
 - reference attributes 176
 - semantic types 190
 - text search 202
 - database connection parameter file
 - locating 585
 - parameters 75
 - database ID
 - deleting 434
 - database indexes
 - automatically-created 199
 - creating 198
 - defining default table spaces 167, 168
 - viewing 200
 - database passwords
 - changing for resource manager 434
 - database schema, locating 592

- databases
 - analyzing DB2 for optimization 395
 - managing 394
 - optimizing 395
 - switching 118
- DB2
 - administration authority 429
 - authentication for passwords 432
 - connecting with a shared ID 430
- DB2 Configuration Assistant 72
- DB2 Content Manager OnDemand server
 - troubleshooting sockets 37
- DB2CON 17
- DB2UserID 25
- deadlock 609
- decision points (document routing),
 - creating 307
- decision points (document routing),
 - description 309
- default table spaces
 - for components and indexes 167, 168
- delete rule 165
- dependent definitions 218
- device manager
 - modifying with retention protection 345
- device managers
 - by operating system or product 328
 - copying 329
 - creating 325
 - deleting 329
 - description 326
 - disabled 326
 - ICMZFS 326
 - modifying 328
 - TSMPOOLED 327
 - viewing 328
- DGL0303A error 590
- DGL2616A error 651
- DGL3804 error 664
- DGL5203A error 611
- DGL5390A error 608
- DGL7186A error 635
- directory, installation 571
- disability
 - accessibility features of graphical process builder 303
 - accessibility features of IBM Content Manager products 1
- disk
 - replacing or repartitioning 347
 - replacing the staging volume
 - on UNIX 347
 - on Windows 348
 - replacing the storage volume
 - on UNIX 348
 - on Windows 349
- display names
 - defining 149
 - description 107
- display results, defining 98
- display, accessible 3
- document formats 108
- document management
 - defining relations 171
- document model 160
- document part
 - classification 160
 - definition 160
 - example 142
 - ICMANNOTATION type 160
 - ICMBASE type 160
 - ICMBASESTREAM type 160
 - ICMBASETEXT type 160
 - ICMNOTELOG type 160
 - version policies 157
- document routing
 - access control lists
 - designing 265
 - example 268
 - accessibility features of graphical builder 303
 - action lists
 - copying 275
 - creating 274
 - description 274
 - modifying 274
 - viewing 274
 - actions
 - copying 272
 - creating 269
 - description 270
 - modifying 271
 - viewing 271
 - ad hoc routing, description 305
 - automatic, establishing 317
 - business applications
 - copying 293
 - defining 291
 - deleting 294
 - modifying 293
 - viewing 293
 - collection points
 - copying 289
 - creating 283
 - deleting 294
 - description 285
 - modifying 286
 - viewing 286
 - comparison with IBM Information Integrator for Content advanced workflow 249
 - creating item types for 265
 - decision points, creating 307
 - decision points, description 309
 - example
 - planning item types 259
 - planning privileges 262
 - planning process flow 256
 - planning user roles 258
 - planning variables 264
 - planning worklists 260
 - privilege groups for item types 267
 - privilege groups for work nodes 268
 - privilege groups for worklists 268
 - graphical process builder
 - modeling processes with 294
 - tools 301
 - overview illustration of
 - creating a 254
 - planning for 253
- document routing (*continued*)
 - parallel routes
 - creating 310
 - description 304, 311
 - prerequisite tasks 265
 - privileges, planning 262
 - process
 - builder, accessibility and 303
 - builder, customizing 299
 - processes
 - associating as a subprocess 305
 - connecting steps in 306
 - copying 298
 - creating 295
 - creating, overview 265
 - deleting 299
 - description 295
 - exporting as XML text 312
 - importing from XML text 296
 - modifying 297
 - planning flow 256
 - planning user roles 258
 - planning, overview 256
 - printing diagram 312
 - updating 304
 - verifying 311
 - viewing 297
 - sample, insurance scenario 267
 - subprocesses, creating 305
 - variables
 - basing decisions on 307, 309
 - creating for a collection point 283
 - creating for a work basket 276
 - planning 264
 - virtual nodes, description 304
 - work baskets
 - copying 281
 - creating 276
 - deleting 294
 - description 278
 - modifying 279
 - viewing 279
 - work nodes
 - adding to a process 304
 - creating inside builder 304
 - creating outside of builder 276
 - description 276
 - work packages, description 314
 - work steps, description 305
 - worklists
 - copying 316
 - creating 312
 - deleting 317
 - description 314
 - modifying 315
 - planning 260
 - viewing 315
- domains
 - assigning
 - a collection to 520
 - a resource manager to 520
 - user group to 520
 - users to 520
 - description 517
 - moving
 - a collection 522
 - access control lists between 522

- domains (*continued*)
 - moving (*continued*)
 - privilege sets between 523
 - users across 521
 - subadministrator privileges 517
 - superadministrator privileges 517
- dsntrace
 - DB2-related problems 414
 - enabling 414
 - example 414
 - Web server procedure 414
- dynamic log configuration 398

E

- eClient
 - accessibility 4
 - action list, description 274
 - action, creating 269
 - ad hoc routing 305
 - connectors display in 306
 - notification flag 295
 - worklist
 - description 314
 - planning 260
- EIPAdminEntity privilege 483
- EIPAdminServer privilege 483
- EIPAdminTemplate privilege 483
- EIPAdminTextEntity privilege 483
- encryption key, synchronizing 639
- environment variable 571
- event codes 416
- event handler
 - cmbemconfig.properties 696
 - modifying settings 696
- event logging 414
- event monitor
 - cmbemconfig.properties 696
 - modifying settings 696
 - starting 698
 - stopping 698
 - troubleshooting
 - cmbemconfig.properties 599, 600
 - database error 598
 - initial context 598
 - LDAP authentication 599
 - starting 597
- event nodes
 - IBM Information Integrator for Content workflow
 - creating 554
 - description 555
- event subscriptions 701
 - defining 702, 704
 - event subscriptions
 - deleting 704
 - updating 704
- event tables
 - description 418
 - maintaining 415
 - removing entries 415
 - searching 416
- events
 - subscribing to 701, 702, 704
- exit condition connectors (IBM Information Integrator for Content workflow), creating 556

- exit programs, z/OS 396
- export options 218

F

- federated attributes
 - adding to a federated entity
 - manually 86
 - with the wizard 80
 - creating 86
 - modifying 87
 - viewing 87
- federated attributes properties, defining
 - with the wizard 82
- federated entities
 - associating to a federated text
 - index 91
 - copying 90
 - creating
 - manually 83
 - using the wizard 79
 - deleting definitions 100
 - description 88
 - mapping 87
 - modifying
 - manually 89
 - with the wizard 82
 - viewing 89
- federated folders
 - description 89
- Federated searches
 - overview 79
- federated text index
 - copying 91
 - creating 90
 - deleting definitions 100
 - modifying 91
 - viewing 91
- file permissions
 - on resource manager objects 321
- file system volumes on UNIX
 - copying 337
 - creating 335
 - deleting 347
 - modifying 336
 - viewing 336
- file system volumes on Windows
 - copying 335
 - creating 333
 - deleting 347
 - modifying 334
 - viewing 334
- FileNet Business Process Manager
 - example configuration 686
 - integration 683
 - steps 683
 - with Oracle library server 688
 - overview of integration with IBM Content Manager 683
- FileNet Business Process Manager integrated with IBM Content Manager 249
- First Steps
 - launching in IBM Content Manager 104
- foreign keys
 - adding 178

- foreign keys (*continued*)
 - description 181
 - example 142
 - scope 173

G

- general integration 704
- graphical process builder, document routing
 - launching 294
 - tools 301
- graphical workflow builder, IBM Information Integrator for Content
 - launching 540
 - table 539
 - tools 538

H

- hard disk
 - replacing or repartitioning 347
 - replacing the staging volume
 - on UNIX 347
 - on Windows 348
 - replacing the storage volume
 - on UNIX 348
 - on Windows 349
- HFS file 406
- HTTP Server
 - enabling trace facility 414

I

- IBM Support Assistant 566
 - data collected by 568
- IBMCMROOT 571
- ICMCONCT 467
- ICMMRMWS 413
- ICMROOT 571
- ICMSERVER.LOG, default for library server trace 408
- ICMSERVERREPTYPE 660
- ICMSTCompiledACL
 - space-optimized ACL mode 25, 27, 29
 - time-optimized ACL mode 25, 27, 29
- ICMSTITEMEVENTS
 - event logging 414
 - removing entries 415
 - searching 416
- ICMSTNLSKEYWORDS 414
- ICMSTSYSADMEVENTS
 - event logging 414
 - removing entries 415
 - searching 416
- ICMSTSYSCONTROL library server control table, tracing parameters 406, 411
- ImagePlus for OS/390 server
 - tracing 35
- importing users with LDAP 456
- index
 - reorganizing 204
 - updating 204, 211
- index class 165

- index update settings 202, 209
- information center
 - cmic commands not found 575
 - conflict with other Windows applications 576
 - information center readme file link does not work 573
 - information center will not start with eClient 575
 - main eClient help topic not found 574
 - page not found 574
 - topic appears in English 572
 - welcome page not found 573
- installation
 - verification
 - resource manager for z/OS 393
- insurance scenario 142
- integration
 - event monitor and event handler settings 696
 - JMS queue setup 688
 - JMS queue setup with LDAP 690, 692
 - logging on to FileNet Business Process Manager 695
 - setting up the connection 694
- item type
 - adding attributes 163
 - auto-linking 187
 - copying 173
 - database indexes 199
 - defining 153
 - deleting 173
 - example 142
 - invalid parameter error for Start on process field 590
 - logging events 170
 - modifying 172
 - overview 156
 - selecting an access control list 162
 - specifying default storage 170
 - subset 201
 - view 201
 - viewing 172
- item type classification
 - document 160
 - document part 160
 - item 159
 - resource item 159
- item type subsets
 - copying 202
 - creating 200
 - modifying 201
 - viewing 201
- item types
 - child components 165
 - creating for document routing 265
 - planning for document routing 259
 - problem exporting to WSDL 605
 - root components 165
- ItemAdd privilege 484, 493
- ItemAddLink privilege 484
- ItemAddToDomain privilege 484
- ItemCheckInOut privilege 484
- ItemDelete privilege 484, 493
- ItemDeletePart privilege 484

- ItemGetAssignedWork privilege 484, 493
- ItemGetWork privilege 484, 493
- ItemGetWorkList privilege 484, 493
- ItemLinked privilege 484
- ItemLinkTo privilege 484
- ItemMove privilege 484
- ItemQuery privilege 484
- ItemRecordsAdmin privilege 484
- ItemRemoveLink privilege 484
- ItemRoute privilege 484, 493
- ItemRouteEnd privilege 484, 493
- ItemRouteStart privilege 484, 493
- items
 - classifying as an item type 159
 - version policies 157
- ItemSetSysAttr privilege 484, 493
- ItemSetUserAttr privilege 484, 493
- ItemSQLSelect privilege 484
- ItemSuperAccess privilege 484
- ItemSuperCheckIn privilege 484
- ItemTypeQuery privilege 484
- ItemUpdateWork privilege 484, 493

J

- JDBC, error message 664
- JMS
 - troubleshooting
 - LDAP authentication 599
- journal article scenario 140

K

- key field 149
- keyboard
 - drawing with in graphical process builder 303
 - navigation and input features 1
 - shortcuts 2

L

- LAN cache
 - description 51
 - enabling 48
 - relationship to resource manager 41
- language codes 13
- language definitions
 - additional 14
 - creating 12
 - deleting 16
 - description 12
 - modifying 15
 - viewing 15
- LDAP 599
 - creating the key database file 453
 - defining configuration 438
 - defining import schedule 444
 - description 435
 - enabling Secure Sockets Layer 453
 - filtering users 449
 - generating the cmbcenv.properties file 437
 - identify the LDAP Directory Source 450

LDAP (*continued*)

- importing users 444
- importing users from 456
- installing prerequisites for LDAP authentication 452
- installing the cmbcenv.properties file on the library server 442
- installing the cmbcenv.properties file on the resource manager 443
- installing the user exit 451
- integrating with Content Manager EE 436
 - Step 1. verifying prerequisites 437
 - Step 10. validating an LDAP logon with the clients 456
 - Step 2. generating the properties file 437
 - Step 3. testing the connection 441
 - Step 4. installing the properties file on the library server 442
 - Step 5. installing the properties file on the resource manager 443
 - Step 6. importing users with the LDAP user import utility 444
 - Step 7. installing the user exit 451
 - Step 8. installing prerequisites for LDAP authentication 452
 - Step 9. enabling Secure Sockets Layer 453
- Secure Sockets Layer 453
- testing the connection 441
- troubleshooting 666
 - connection problems after user import 674
 - finding log files for 666
 - LDAP import utility schedule on non-English systems 669
 - permissions to run the LDAP user import utility 668
 - resource manager
 - authentication 672
 - scheduled import failure 670
 - scheduler save function fails 669
 - user authentication 674
- usage notes 449
- user authentication prerequisites
 - Global Security Kit 452
 - GSKit 452
 - IBM Tivoli Directory Server client 452
- using the LDAP user import utility 444
- validating an LDAP logon with the clients 456
- verifying prerequisites 437
- library server
 - backing up data 368
 - changing password 119
 - configuration
 - defaults 10
 - features 8
 - log and trace information 10
 - modifying 6
 - parameters 6
 - SSL communication with the LDAP server 455
 - viewing 6

- library server *(continued)*
 - connecting the system administration client 67
 - deferring data model change execution 241
 - deferring data model change execution for Oracle 246
 - description 6
 - event table log 418
 - fail-over 366
 - interaction with resource manager 41
 - list of users logged on 434
 - locating connection information
 - UNIX 68
 - Windows 68
 - z/OS 68
 - manually connecting the system administration client
 - cataloging the DB2 node and database on UNIX and Windows 73
 - cataloging the DB2 node and database on z/OS 73
 - connecting to a DB2 library server 72
 - database cataloging variables 74
 - DB2 Configuration Assistant 72
 - password reference 662
 - pausing for backups 368
 - resuming after backups 369
 - server configuration utility 70
 - single sign-on 6
 - trace facility 410
 - troubleshooting overview 600
 - trusted logon 6
- library server monitor fail-over service 366
- link type
 - copying 175
 - defining 174
 - deleting 176
 - viewing 175
- links
 - auto-linking 188
 - description 174
 - example 142
 - link types 174
 - scope 173
- Lithuanian locale considerations 682
- lock contention 609
- log and trace information
 - modifying 10
 - viewing 10
- log files
 - log file locations 570
- logging 397
- logging and tracing components 396
- logging and tracing utility
 - beans 404
 - C++ APIs 404
 - Java APIs 403
 - LDAP user import utility 399
 - library server 400
 - resource manager 400
 - system administration client 399
- Logging and tracing utility 397

- login user exit 17
- login user exit scenarios
 - overview 17
- logs
 - server inventory 84

M

- mapping attributes 81
- media archive volumes
 - copying 342
 - creating 341
 - deleting 347
 - modifying 341
 - viewing 341
- media archive, password reference 662
- media object (XDO) class
 - copying 197
 - creating 195
 - deleting 198
 - description 195
 - modifying 197
 - viewing 197
- media resource manager 339
- media server 339
- migration
 - changing date 355
 - creating a policy 352
 - migrating and purging DB2 Content Manager VideoCharger Server objects 355
 - policies 352
 - schedule 355
 - scheduling 58
 - threshold 352
- migration policies
 - copying 354
 - creating 352
 - creating entries 354
 - deleting 354
 - description 352
 - modifying 353
 - modifying entries 354
 - viewing 353
 - viewing entries 354
- migrator 352
- MIME types
 - adding an editor 101
 - adding for servers 100
 - defining 192
 - description 193
 - modifying 194
 - overview 100
 - setting up an association 101
 - viewing 194
- modeling data
 - adding data to Content Manager 136
 - deciding to create a custom data model 135
 - diagramming your data relationships 134
 - identifying
 - data 125
 - elements that might be searched for 132
 - hierarchies and elements that might have multiple values 133

- modeling data *(continued)*
 - identifying *(continued)*
 - users and what data they need to access 131
 - separating your data into operational and non-operational data 127
 - sorting your data into like types 129
- MQ Workflow server
 - synchronizing users and groups with
 - adding or updating 530
 - deleting 530
 - failed to add or update 677
 - troubleshooting 676
- multi-valued attributes 165

N

- NAS 332
- native attribute
 - overview 87
- native attributes, viewing 87
- native entities, viewing 87
- native entity
 - overview 89
- network-attached storage
 - creating 331
 - description 332
- No privs privilege set 509
- nodes
 - IBM Information Integrator for Content
 - collection node 553
 - description 545
 - event 554
 - start 547
 - stop 548
 - sub-workflow 552
 - user exit routine 549
 - value 550
 - work 546

O

- OAM collections 357
- object server 41
- object storage
 - cataloging resource manager objects 367
 - creating
 - collections 356
 - device managers 325
 - migration policies 352
 - migration policy entries 354
 - storage classes 323
 - storage groups 350
 - storage systems 329
 - description 320
 - load balancing 321
 - managing 319
 - setting up replication 362
- objects
 - cataloging resource manager objects 367
 - definition 192
 - file permissions 321
 - importing 221

OITOPTIONFLAG system configuration parameter 209
 Oracle
 administration authority 430
 authentication for passwords 433
 connecting with a shared ID 430
 troubleshooting 602

P

parallel processing
 document routing
 creating 310
 description 295, 311
 IBM Information Integrator for Content workflow
 creating 545
 description 541
 parallel routes
 document routing
 creating 310
 description 304, 311
 IBM Information Integrator for Content workflow
 creating 545
 description 541
 passwords
 changing
 resource manager database access 434
 ICMCONCT account 662
 library server, changing 119
 managing 429
 reference 662
 resetting user accounts 461
 resource manager, changing 16
 restrictions for DB2
 authentication 432
 restrictions for Oracle
 authentication 433
 path, installation 571
 PAUSESERVER utility, description 368
 port number
 access type 53
 changing
 on UNIX and Windows 637
 on z/OS 638
 prefetch
 description 45
 privilege groups
 copying 516
 creating 513
 deleting 516
 description 514
 modifying 515
 predefined 514
 selecting for document routing
 example
 item types 267
 work nodes 268
 worklists 268
 viewing 515
 privilege sets
 assigning to access control lists 513
 copying
 advanced 512
 basic 512

privilege sets (*continued*)
 creating 507
 advanced 508
 basic 508
 definition 507
 deleting 513
 modifying
 advanced 511
 basic 511
 moving between domains 523
 predefined
 ClientUserAllPrivs 509
 ClientUserCreateandDelete 509
 ClientUserEdit 509
 ClientUserReadOnly 509
 No privs 509
 SysAdminCM 509
 SysAdminEIP 509
 SysAdminSubDomainCM 509
 SysAdminSubDomainEIP 509
 SysAdminSuper 509
 UserDBConnect 509
 UserDBTrustedConnect 509
 viewing
 advanced 511
 basic 511
 privileges
 AllowConnectToLogon 478
 AllowTrustedLogon 478
 assigning 94
 ClientAddNewBasePart 478
 ClientAddToNoteLog 478
 ClientAdvancedSearch 478
 ClientDeleteBasePart 478
 ClientExport 478
 ClientGetWorkList 478
 ClientImport 478
 ClientModifyAnnotation 478
 ClientModifyBasePart 478
 ClientModifyNoteLog 478
 ClientPrint 478
 ClientReadAnnotation 478
 ClientReadBasePart 478
 ClientReadHistory 478
 ClientReadNoteLog 478
 ClientScan 478
 copying 506
 creating 477
 deleting 507
 description 467
 document routing, planning 262
 domain subadministrator 517
 domain superadministrator 517
 EIPAdminEntity 483
 EIPAdminServer 483
 EIPAdminTemplate 483
 EIPAdminTextEntity 483
 IBM Information Integrator for Content 483
 ItemAdd privilege 484, 493
 ItemAddLink privilege 484
 ItemAddToDomain privilege 484
 ItemCheckInOut privilege 484
 ItemDelete privilege 484, 493
 ItemDeletePart privilege 484
 ItemGetAssignedWork privilege 484, 493

privileges (*continued*)
 ItemGetWork privilege 484, 493
 ItemGetWorkList privilege 484, 493
 ItemLinked privilege 484, 493
 ItemLinkTo privilege 484
 ItemMove privilege 484
 ItemQuery privilege 484
 ItemRecordsAdmin privilege 484, 493
 ItemRemoveLink privilege 484
 ItemRoute privilege 484, 493
 ItemRouteEnd privilege 484, 493
 ItemRouteStart privilege 484, 493
 ItemSetSysAttr privilege 484, 493
 ItemSetUserAttr privilege 484, 493
 ItemSQLSelect privilege 484
 ItemSuperAccess privilege 484
 ItemSuperCheckIn privilege 484
 ItemTypeQuery privilege 484
 ItemUpdateWork privilege 484
 modifying 506
 predefined 477
 groups 514
 privilege sets 509
 SystemBatchCompileACL privilege 497
 SystemDefineACL privilege 497
 SystemDefineAttrs privilege 497
 SystemDefineDomain privilege 497
 SystemDefineGroup privilege 497
 SystemDefineItemType privilege 497
 SystemDefineLinkType privilege 497
 SystemDefineMimeType privilege 497
 SystemDefineNewKywdClass privilege 497
 SystemDefineNLSLang privilege 497
 SystemDefinePrivs privilege 497
 SystemDefineRM privilege 497
 SystemDefineSemanticType privilege 497
 SystemDefineSMSColl privilege 497
 SystemDefineUser privilege 497
 SystemDefineXdoObject privilege 497
 SystemDomainAdmin privilege 497
 SystemDomainQuery privilege 497
 SystemGetKey privilege 497
 SystemGrantUserPrivs privilege 497
 SystemManageKey privilege 497
 SystemQueryAllKywdClass privilege 497
 SystemQueryGroup privilege 497
 SystemQueryOtherDomains privilege 497
 SystemQueryUserPrivs privilege 497
 SystemSetACL privilege 497
 SystemSetCtrlParm privilege 497
 SystemSetGrantPrivs privilege 497
 SystemSetReplicaRule privilege 497
 SystemSuperDomainAdmin privilege 497
 viewing 506
 WFSuperWorkFlowPriv 505
 WFWorklist 505

- process builder, graphical (document routing)
 - customizing display and behavior 299
 - keyboard instead of mouse 303
- process integration 702
- processes
 - document routing
 - copying 298
 - creating 295
 - creating, overview 265
 - deleting 299
 - description 295
 - exporting as XML text 312
 - importing from XML text 296
 - modifying 297
 - planning flow 256
 - planning user roles 258
 - planning, overview 256
 - prerequisite tasks 265
 - printing diagram 312
 - updating 304
 - verifying 311
 - viewing 297
- IBM Information Integrator for Content workflow
 - checking in 558
 - checking out 542
 - copying definition 543
 - creating 540
 - description 541
 - modeling 537
 - modifying definition 542
 - releasing 558
 - verifying 557
 - viewing definition 542

Q

- query performance 602

R

- reference attributes
 - copying 178
 - creating 176
 - deleting 178
 - description 176
 - example 142
 - modifying 177
 - scope 173
 - viewing 177
- replication
 - default options 10
 - defining rules for administrative domains 366
 - description 364
 - library server monitor fail-over service 366
 - options 357
 - scheduling 59
 - setting up 362
 - stored objects 365
 - troubleshooting
 - checked out items not replicated 648
- replication (*continued*)
 - troubleshooting (*continued*)
 - migrated items not replicated 650
 - new rules not taking effect 651
 - return code 7400 648
 - rules in the public domain 649
- resource manager
 - adding
 - access types 53
 - server definitions 61
 - assigning to a domain 520
 - assigning users to 464
 - background services 44
 - backing up data 368
 - cataloging objects 367
 - changing
 - owner 375, 376
 - passwords 16
 - port number on UNIX and Windows 637
 - port number on z/OS 638
 - configuration
 - activating 56
 - copying 60
 - creating 56
 - deleting 61
 - modifying 60
 - planning 60
 - setting cycles 57
 - setting migrator schedule 58
 - setting replicator schedule 59
 - setting services 58
 - viewing 60
 - configuring 41
 - SSL communication with the LDAP server 455
 - copying a server definition 63
 - defining
 - additional resource managers 41
 - configuration 56
 - OAM collections 357
 - UNIX or Windows resource manager 48
 - z/OS resource manager 50
 - deleting a server definition 63
 - description 41
 - exit programs on z/OS 396
 - interaction with library server 41
 - lockout 65
 - releasing 66
 - marking off-line
 - UNIX and Windows resource managers 48
 - z/OS resource managers 50
 - marking offline 636
 - marking online 636
 - modifying
 - access types 53
 - properties 52
 - staging area properties 54
 - modifying a server definition 63
 - moving from one domain to another 522
 - objects
 - file permissions 321
 - password reference 662
 - prefetch 45

- resource manager (*continued*)
 - protocol 53
 - reasons for restarting 371
 - selecting a default 464
 - starting or stopping
 - behavior 375
 - on AIX 372
 - on Linux 372
 - on Solaris 373
 - on Windows 374
 - on z/OS 375
 - testing SSL connection 47
 - Tivoli Storage Manager collections on z/OS 358
 - trace facility 410, 412
 - troubleshooting
 - asynchronous jobs 643, 644, 645
 - ChangeSMS failure 649
 - database connection failures 645, 646
 - LDAP authentication 672
 - overview 628
 - viewing
 - access types 53
 - properties 52
 - staging area properties 54
 - viewing a server definition 63
 - z/OS resource managers
 - availability 46
 - differences between z/OS version and UNIX or Windows version 44
 - features and limitations specific to z/OS 44
 - functions not supported on z/OS 45
 - scalability 46
- resource manager for z/OS
 - installation
 - verification 393
 - library server tables
 - cleanup 393
 - validating data 393
 - validation utilities 393
- resource manager log files
 - configuring 405
 - levels of logging 405
- resource manager services
 - starting and stopping 376
- RESUMESERVER utility, description 369
- return codes, SQL 410
- RMSTAGING
 - replacing on UNIX 347
 - replacing on Windows 348
- root components, description 165
- routes
 - IBM Information Integrator for Content workflow
 - collection event lists 555
 - exit condition 556
 - parallel 545
 - parallel in document routing 310, 311

S

- schema name, finding 68

- search criteria
 - copying 99
 - creating
 - manually 96
 - with the wizard 92
 - modifying 99
 - view 99
- search settings
 - defining default
 - manually 97
 - with the wizard 94
- search template
 - access to 94
 - creating
 - manually 95
 - with the wizard 92
 - defining default values 97
 - deleting definitions 100
 - description 91
 - modifying
 - manually 99
 - with the wizard 95
 - viewing 98, 99
- Secure Socket Layer
 - testing 47
 - troubleshooting 635
- Secure Sockets Layer (SSL)
 - LDAP 453
- security
 - Global Security Kit, enabling 452
- semantic types
 - copying 191
 - defining 190
 - definition 190
 - deleting 192
 - predefined semantic types 190
 - viewing 191
- SEMANTICTYPE 602
- server configuration utility
 - description 70
 - field descriptions 71
 - starting on UNIX 70
 - starting on Windows 70
- server definition
 - adding 61
 - adding content encryption 64
 - Content Manager for AS/400 38
 - Content Manager OnDemand 36
 - copying 63
 - defining your own 31
 - deleting 63
 - description 62
 - IBM Content Manager Version 8 34
 - ImagePlus for OS/390 35
 - modifying 63
 - viewing 63
- server inventory 32
 - filtering 84
 - logs 84
 - refreshing 83
 - viewing 83
- server type definitions 33
- SERVERREPTYPE
 - DB2 17
 - DB2CON 17
- servers
 - backing up data 368
- servers (*continued*)
 - configuring
 - library server 5
 - resource manager 56
 - server definitions 61
 - deleting definitions 100
 - managing 371
 - restoring data 368
- services
 - IBM Information Integrator for
 - Content workflow, enabling 529
 - Windows
 - information center 576
 - library server monitor
 - fail-over 366
- services, setting 58
- shared connection ID 25
- shared database connection ID
 - changing 431
 - creating 430, 431
- shortcut keys 2
- single sign-on
 - description 11
 - enabling 6
 - WebSphere security 11
- SMS interface utility processing
 - error 640
- SQL return codes 410
- SQL0302N error 614
- SQL0334N error 607
- SQL0911N error 609
- SSL
 - testing 47
 - troubleshooting 635
- SSL communication
 - configuring the system administration
 - client 454
 - library server
 - configuring communication with
 - the LDAP server 455
 - resource manager
 - configuring communication with
 - the LDAP server 455
- staging area
 - description 55
 - modifying 54
 - relationship to resource manager 41
 - viewing 54
- staging volume
 - replacing on UNIX 347
 - replacing on Windows 348
- start nodes
 - document routing 304
 - IBM Information Integrator for
 - Content workflow, creating 547
- stop nodes
 - document routing 304
 - IBM Information Integrator for
 - Content workflow, creating 548
- storage classes
 - copying 324
 - creating 323
 - deleting 325
 - description 323
 - modifying 324
 - viewing 324
- storage groups
 - copying 351
 - creating 350
 - deleting 351
 - description 350
 - modifying 351
 - viewing 351
- storage management
 - collections 360
 - default options 10
 - device managers 326
 - migration policies 352
 - storage classes 323
 - storage groups 350
 - storage systems 329, 338
- storage systems
 - assignments 329, 338
 - availability by operating system 329, 338
 - creating
 - file system volumes on UNIX 335
 - file system volumes on
 - Windows 333
 - media archive volumes 341
 - network-attached storage 331
 - Tivoli Storage Manager 342
 - Tivoli Storage Manager with
 - retention protection 343
 - VideoCharger volumes 338
 - deleting 347
 - description 329, 338
 - volume 333
- storage volume
 - replacing on UNIX 348
 - replacing on Windows 349
- storage, default options 10
- sub-workflow nodes (IBM Information Integrator for Content workflow),
 - creating 552
- subprocesses, creating in document
 - routing 305
- summary table, IBM Information Integrator for Content workflow
 - description 539
 - launching 540
- supported document formats 108
- SysAdminCM privilege set 509
- SysAdminEIP privilege set 509
- SysAdminSubDomainCM privilege
 - set 509
- SysAdminSubDomainEIP privilege
 - set 509
- SysAdminSuper privilege set 509
- SYSPRINT 406
- system administration client
 - configuring for SSL
 - communication 454
 - connecting to administration
 - database 67
 - connecting to library server 67
 - connecting to remote administration
 - database 67
 - connecting to remote library
 - server 67
 - description 106
 - First Steps introduces
 - IBM Content Manager 104

- system administration client *(continued)*
 - logging on 117
 - manually connecting to DB2
 - administration database
 - overview 72
 - manually connecting to DB2 library server 72
 - cataloging the DB2 node and database on UNIX and Windows 73
 - cataloging the DB2 node and database on z/OS 73
 - cataloging variables 74
 - DB2 Configuration Assistant 72
 - server configuration utility 70
 - setting location of trace log 408
 - setting the trace level 408
 - starting on UNIX 117
 - starting on Windows 117
 - switching databases 118
 - troubleshooting field-level help 579
 - troubleshooting Help button 579
 - troubleshooting startup
 - on UNIX 582
 - on Windows 582
 - views 106
- SystemBatchCompileACL privilege 497
- SystemDefineACL privilege 497
- SystemDefineAttrs privilege 497
- SystemDefineDomain privilege 497
- SystemDefineGroup privilege 497
- SystemDefineItemType privilege 497
- SystemDefineLinkType privilege 497
- SystemDefineMimeType privilege 497
- SystemDefineNewKywdClass privilege 497
- SystemDefineNLSTLang privilege 497
- SystemDefinePrivs privilege 497
- SystemDefineRM privilege 497
- SystemDefineSemanticType privilege 497
- SystemDefineSMSColl privilege 497
- SystemDefineUser privilege 497
- SystemDefineXdoObject privilege 497
- SystemDomainAdmin privilege 497
- SystemDomainQuery privilege 497
- SystemGetKey privilege 497
- SystemGrantUserPrivs privilege 497
- SystemManageKey privilege 497
- SystemQueryAllKywdClass privilege 497
- SystemQueryGroup privilege 497
- SystemQueryOtherDomains privilege 497
- SystemQueryUserPrivs privilege 497
- SystemSetACL privilege 497
- SystemSetCtrlParm privilege 497
- SystemSetGrantPrivs privilege 497
- SystemSetReplicaRule privilege 497
- SystemSuperDomainAdmin privilege 497

T

- tabular workflow builder, IBM
 - Information Integrator for Content
 - description 539

- tabular workflow builder, IBM
 - Information Integrator for Content
 - (continued)*
 - launching 540
- text index 216, 627
- text index timeout 217
- text search 211
 - code page requirements for Thai
 - phased text search 613
 - correcting text index failures 205
 - correcting text index failures in DB2
 - for z/OS systems 212
 - enabling 149
 - starting 8
- text search index
 - limiting data extracted 209
- text search indexing
 - resolving problems 216
- text search options
 - coded character set identifier (CCSID)
 - requirements 213
 - defining for DB2 202
 - defining for DB2 for z/OS 209
 - defining for Oracle 215
 - defining for z/OS for DB2 213
 - indexing large objects 207
 - DB2 for z/OS 214
 - limiting data extracted for
 - indexing 209
- Thai locale considerations 682
- Tivoli Storage Manager
 - collections on z/OS 358
 - password reference 662
 - using to back up and restore data 368
- Tivoli Storage Manager volumes
 - copying 346
 - creating 342
 - deleting 347
 - modifying 345
 - retention protection 343
 - viewing 345
- tnsnames.ora 68
- trace facility
 - Content Manager for z/OS 412, 413
 - HTTP Server, enabling 414
 - library server
 - enabling 408
 - trace levels 406, 411
 - resource manager 412, 413
 - enabling 414
 - enabling by using the system
 - administration client 412
 - enabling dynamically 413
 - trace levels 413, 414
- trace file name 408
- trace level
 - specifying 406
- trace levels
 - Content Manager for z/OS,
 - setting 412
 - Content Manager for z/OS,
 - viewing 412
 - library server 406
 - resource manager 412, 413

- trace values
 - defining
 - defining DB2 408
 - defining Oracle 409
 - trace values
 - disabling DB2 408
 - disabling Oracle 409
- transaction correlation
 - cminstall.log 398
- troubleshooting 599
 - access control lists 659
 - administration client messages 579
 - Auto-linking a race condition creates
 - duplicate folders 595
 - BLOB and CLOB size limitations
 - SQL0302N error 614
 - cannot log on to z/OS 589
 - changing the resource manager port
 - number
 - on UNIX and Windows 637
 - on z/OS 638
 - client logon errors
 - after installing fix pack 589
 - logon failure 584
 - cmbwfstart failure 676
 - connection errors 590
 - CTE0143 error 610
 - database connections 634
 - database creation 632
 - database deployment 632
 - DB2 Content Manager V7.1
 - server 652
 - DGL0394A 593
 - DGL2616A error 651
 - DGL3804 error 664
 - DGL5203A error 611
 - DGL5390A error 608
 - DGL7186A error 635
 - DKDDO.fromXML() 610
 - document routing 679, 680
 - dsntrace 414
 - EIPUser2WF.bat failure 677
 - error updating user 664
 - information center
 - cmic commands not found 575
 - conflict with other Windows
 - applications 576
 - does not display on UNIX 572
 - information center readme file link
 - does not work 573
 - information center will not start
 - with eClient 575
 - Java error starting information
 - center 576
 - main eClient help topic not
 - found 574
 - page not found 574
 - topic appears in English 572
 - welcome page not found 573
 - invalid password when updating text
 - indexes 202
 - inventory viewer problems 591
 - item creation 607
 - item retrieval 607
 - item type definition 611
 - item type synchronization errors 172

troubleshooting (continued)

- JAR file clash between WebSphere Application Server and XML service 596
- languages 681
- LDAP
 - account lockouts 675
 - connection problems after user import 674
 - resource manager authentication failure 672
 - scheduled import failure 670
 - user authentication failure 670
- LDAP user import scheduler fails to create CRON job 669
- library server 600
 - return code 7652 650
- locales 681
- locked accounts 660
- log and trace 654
- maximum cursors 607
- missing entities and search templates 593
- overview 565
- RC=-911 609
- replication
 - checked out items not replicated 648
 - migrated items not replicated 650
 - return code 7400 648
- replication rules
 - new rules not taking effect 651
 - rules in the public domain 649
- resource manager 628
 - asynchronous jobs 643, 644, 645
 - ChangeSMS failure 649
 - database connection failures 645, 646
 - LDAP authentication 672
- resource manager availability 635
- resource manager database creation 632
- resource manager deployment 633
- SQL0334N error 607
- SQL0911N error 609
- SSL 635
- system administration client logon fails 584
- tracing errors 571
- Web server communication 634
- XML Import using process
 - interactively option 595
- XML schema mapping 625
- trusted logon 6, 17
- TSMPOOLED device manager
 - enabling 327
- Turkish locale considerations 682

U

- Unicode problems 607
- updating user error 664
- user
 - passwords 462
- user administrators 469
- user exit routine
 - invocation 24

user exit routines

- IBM Information Integrator for Content workflow nodes,
 - creating 549
 - specifying 172
- user groups
 - assigning 457
 - assigning to a domain 520
 - assigning users 463
 - copying 467
 - creating 464
 - deleting definitions 100
- IBM Information Integrator for Content workflow
 - adding or updating on MQ Workflow 530
 - deleting from MQ Workflow 530
 - managing 465
 - modifying 466
 - moving from one domain to another 522
 - viewing 466
- user IDs
 - creating 432, 433
- IBM Information Integrator for Content workflow
 - adding or updating on MQ Workflow 530
 - deleting from MQ Workflow 530
 - managing 429
 - shared database connection ID 430, 431
- user mapping
 - deleting 459
 - enable 459
 - viewing 459
- user-level tracing 398
- UserDBConnect privilege set 509
- UserDBTrustedConnect privilege set 509
- users
 - access
 - managing 427
 - assigning to a collection 464
 - assigning to domains 520
 - authenticating 429
 - authorization 467
 - copying 460
 - counting 6
 - creating 457
 - current list on library server 434
 - deleting definitions 100
 - importing IDs from LDAP 456
 - managing access 427
 - managing IDs and passwords 429
 - modifying 459
 - moving from one domain to another 521
 - privileges 467
 - viewing 459
- utilities, validation 377, 378

V

- validation utilities
 - description 378
 - discrepancy report 379
 - running recovery tools 384, 389

validation utilities (continued)

- saving discrepancy reports as XML 380
- setting up recovery tools 383
- validation utility
 - running 377
 - scheduling 381
- value nodes (IBM Information Integrator for Content workflow), creating 550
- variables (document routing)
 - basing decisions on 307, 309
 - creating for a collection point 283
 - creating for a work basket 276
 - planning 264
- version policies 157
- VideoCharger
 - creating volumes 338
 - media resource manager 339
 - migrating media objects 355
 - password reference 662
 - purging media objects 355
- VideoCharger volumes
 - copying 340
 - creating 338
 - deleting 347
 - modifying 339
 - viewing 339
- views, switching 118
- virtual nodes (document routing), description 304
- visual process builder, document routing
 - modeling processes with 294
 - tools 301
- visual workflow builder, IBM Information Integrator for Content
 - launching 540
 - table 539
 - tools 538
- volume suspension 338
- volumes 329, 338

W

- WFSuperWorkFlowPriv privilege 505
- WFWorklist privilege 505
- work baskets
 - document routing
 - adding to a process 304
 - copying 281
 - creating 276
 - deleting 294
 - description 278
 - modifying 279
 - viewing 279
- work items (IBM Information Integrator for Content workflow), description 560
- work nodes
 - document routing
 - adding to a process 304
 - business application 292
 - collection point 285
 - copying a business application 293
 - copying a collection point 289
 - copying a work basket 281
 - creating a collection point 283
 - creating a work basket 276

- work nodes (*continued*)
 - document routing (*continued*)
 - creating inside builder 304
 - creating outside of builder 276
 - defining a business application 291
 - deleting a business application 294
 - deleting a collection point 294
 - deleting a work basket 294
 - description 276
 - modifying a business application 293
 - modifying a collection point 286
 - modifying a work basket 279
 - work basket 278
 - IBM Information Integrator for Content
 - creating 546
 - description 547
 - work packages (document routing), description 314
 - work steps (document routing), description 305
 - workflow
 - troubleshooting
 - document routing 680
 - workflow (IBM Information Integrator for Content)
 - access control lists, designing 531
 - action lists
 - copying 537
 - creating 535
 - description 536
 - modifying 536
 - viewing 536
 - actions
 - copying 534
 - creating 532
 - description 533
 - modifying 534
 - viewing 534
 - collection event lists
 - creating 555
 - description 556
 - collection nodes, creating 553
 - collection points
 - creating 553
 - description 553
 - comparison with document routing 249
 - default values, setting 540
 - enabling 529
 - event nodes
 - creating 554
 - description 555
 - exit condition connectors, creating 556
 - graphical process builder
 - table 539
 - tools 538
 - MQ Workflow server
 - adding users on 530
 - deleting users from 530
 - starting 528
 - updating users on 530
 - nodes
 - creating 545
 - description 545
 - overview 525
 - parallel processes
 - creating 545
 - description 541
 - processes
 - checking in 558
 - checking out 542
 - copying definition 543
 - creating 540
 - description 541
 - modeling 537
 - modifying definition 542
 - releasing 558
 - verifying 557
 - viewing definition 542
 - start nodes, creating 547
 - stop nodes, creating 548
 - sub-workflows, creating 552
 - troubleshooting
 - document routing 679
 - MQ Workflow server 676
 - user synchronization 677
 - user exit routine nodes, creating 549
 - user groups
 - adding or updating on MQ Workflow 530
 - deleting from MQ Workflow 530
 - failed to add or update on MQ Workflow 677
 - user IDs
 - adding or updating on MQ Workflow 530
 - deleting from MQ Workflow 530
 - failed to add or update on MQ Workflow 677
 - value nodes, creating 550
 - work items, description 560
 - work nodes
 - creating 546
 - description 547
 - worklists
 - copying 562
 - creating 559
 - description 560
 - modifying 561
 - viewing 561
 - workflow builder
 - IBM Information Integrator for Content
 - launching 540
 - table 539
 - tools 538
 - workflow comparison 249
 - worklists
 - document routing
 - copying 316
 - creating 312
 - deleting 317
 - description 314
 - modifying 315
 - planning 260
 - viewing 315
 - worklists (*continued*)
 - IBM Information Integrator for Content workflow
 - copying 562
 - creating 559
 - description 560
 - modifying 561
 - viewing 561
 - Workload Manager 46
 - WSDL
 - problem exporting an item type 605
- X**
- XML schema mapping 225
 - troubleshooting 625
 - XML text
 - exporting process as 312
 - importing process from 296
- Z**
- ZFS device manager
 - enabling
 - Solaris 326



Product Number: 5724-B19
5697-H60

SC27-1335-12

