IBM Content Manager installation and daily maintenance

Application/Software components:

Table 1.The software required for this content management configuration includes

Client workstation	LMS Server system
DB2 Run-Time Client DB2 Content Manager for Windows® - pClient	AIX 6100-06-05-1115 DB2 Universal Database™ V9.5 HACMP 6.1 IBM HTTP Server V7.0 WebSphere® Application Server V7.0.0.9 Tivoli Storage Manager Server V5.5 Tivoli Storage Manager Client V5.5 DB2 Content Manager library server V8.4.2 DB2 Content Manager resource manager application V8.4.2 DB2 Content Manager resource manager database V9.5 DB2 Content Manager System Administration Client V8.4.2

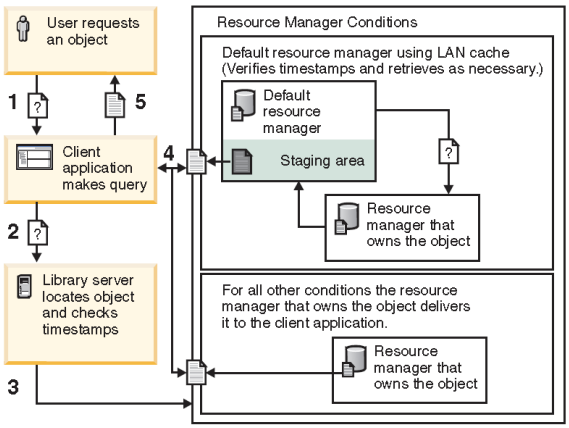
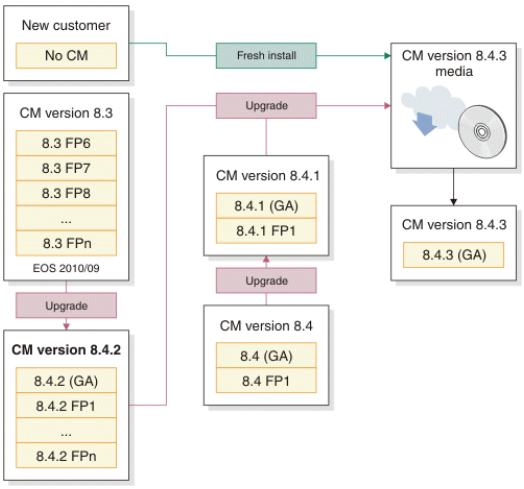


Figure 1. Application/Software components objects logic

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).

```
icmadmin@cm07$  /opt/IBM/db2cmv8/bin/cmlevel
```




```
Products installed:
Content Manager                     + 8.4.02.100 336_840201
Information Integrator for Content  + 8.4.02.100 336_840201
Content Manager eClient             + 8.4.02.100 336_840201

Products configured:
Content Manager                     + 8.4.02.100 336_840201
Information Integrator for Content  + 8.4.02.100 336_840201
Content Manager eClient             + 8.4.02.100 336_840201
```

Installation& configuration

Figure 2. Application/Software components Topology

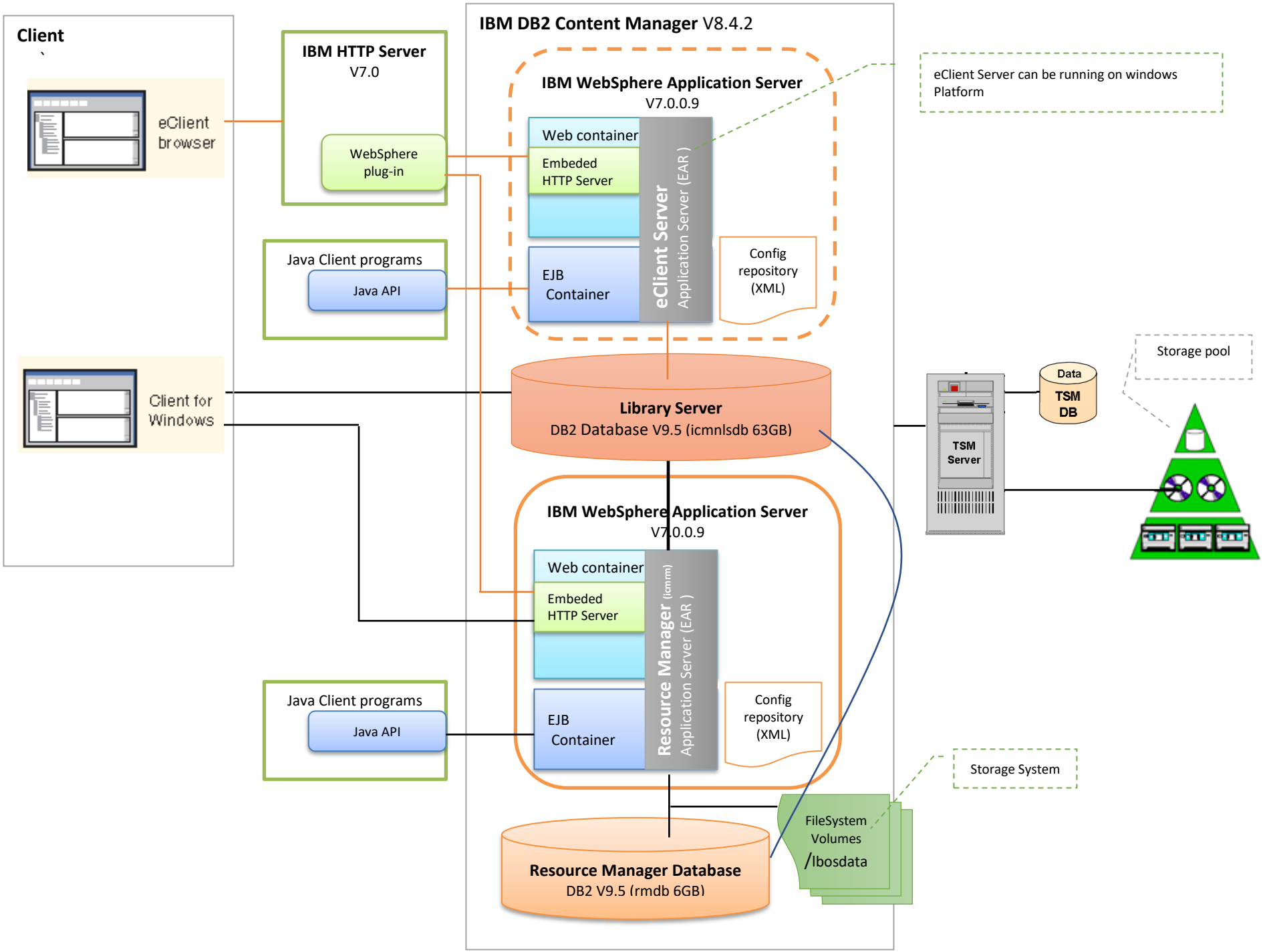


Table 2. Administration and connection IDs

Administration or connection ID	Default name	Actual value here
DB2 Content Manager administration ID	ibmcmadm	ibmcmadm
DB2 Content Manager administration ID password		cmadm83
DB2 Content Manager administrator group	icmadmgrp	icmadmgrp
Library server database administration ID	icmadmin	icmadmin
Library server database administration ID password		cmls83
Database connection ID	icmconct	icmconct
Database connection ID password		cmct83
Resource manager database administration ID	rmadmin	rmadmin
Resource manager database administration ID password		cmrm83
DB2 Universal Database™ instance ID	db2inst1	db2inst1(pw:db2iu82)
	db2inst2	db2inst2(pw:db2iu82)
Primary group of the DB2 Universal Database instance ID	db2admin	db2admin

Table 3. Working directory authentication information

Field name	Description	Default name / option	Actual value here
Administration user name	The name of the DB2 Content Manager administration user.	ibmcmadm	ibmcmadm
Password	If the administration user name exists, the password must match the existing password for the administration user name.		cmadm83
Administration user group	The name of the primary group to which the DB2 Content Manager administration user belongs.	ibmcmgrp	ibmcmgrp

Table 4. Library server

Field name	Description	Field applies to custom installations only	Default name / option	Actual value here
Library server database name	The name of the library server database		icmnlsdb	icmnlsdb
Library server schema name	Identifier used to group tables and database objects	yes	icmadmin	icmadmin
Library server database administration ID	Administration ID for the library server[1]		icmadmin	icmadmin
Password	Password for the library server administration ID[2]		password	passwd

Notes:
If the administration ID already exists on your operating system, type that value in this field and type the corresponding password in the Password field. If it does not exist, the installation program creates it.
You *must* type the password directly in these fields. You cannot copy a password from another area and paste it in the fields.

Table 5. Library server database connection ID

Field name	Description	Default name / option	Actual value here
Library Server connection ID	The database connection ID that is authorized to connect to the library server	icmconct	icmconct
Password	Password for the library server connection ID	password	passwd

Table 6. Library server configuration options

Field name	Description	Default name / option	Actual value here
Name of library server ID	The ID used to identify the library server (Range = 1 to 99)	1	1
Library server transaction ID duration (seconds)	The number of seconds DB2® Content Manager transactions, such as users creating item types, last. This field is similar to a token duration and is used for security purposes.	180	180
Enable Unicode	Select this check box to save characters as Unicode characters. A unicode database is better at handling translated data. You must enable unicode to effectively set up multiple language support through your system administration client. When Unicode is enabled, you then designate code page 1208, which enables UTF-8 Unicode.	selected	yes
Enable text search	Select this check box to enable text search so that users can search the text of stored objects like documents.[1]	cleared	yes
Enable LDAP	Select this check box to manage user IDs and passwords on an enterprise level.[2]	cleared	No

Table 7. Resource manager database

Field name	Description	Field applies to custom installation only	Default name / option	Actual value here
Resource manager database name	The name of the resource manager database		rmdb	rmdb
Resource manager database administration ID	Administration ID for the resource manager[1]		rmadmin	rmadmin
Password	Password for the resource manager administration ID[2]		password	passwd
Resource manager volume mount point	The default storage location of objects that are imported into the resource manager.	yes	C:\	Resource Manager Database Volume mount point: / Resource Manager Database staging directory: /staging

Notes:
If the administration ID already exists on your operating system, type that value in this field and type the corresponding password in the Password field. If it does not exist, the installation program creates it.
You *must* type the password directly in these fields. You cannot copy a password from another area and paste it in the fields.

Table 8. Resource manager options

Field name	Description	Default name / option	Actual value here
Resource manager volume mount point	The default storage location of objects that are imported into the resource manager.	C:\	NO
Resource manager staging area directory	The path where you want to cache objects that are retrieved from the resource manager.	C:\staging	NO

Table 9. Configuring the resource manager application

Field name	Description	Field applies to custom installations only	Default name / option	Actual value here
Application server node name	The node name of your application server, which is typically the short name of this machine. [1] This value is case-sensitive.		Typically, the short name of the machine.	admsrv1
Application server security enabled	Select this check box to indicate that you have previously enabled security for your application server.		cleared	yes
Resource manager Web application name	The name of the Web application that is deployed within your application server	yes	icmrm	icmrm
Resource manager Web application context root	The context root of the resource manager application that is used to construct the Web address to the resource manager Web application.	yes	/icmrm	/icmrm

Token duration	The amount of time in seconds that a token generated by the library server for an action on the resource manager remains active before it is discarded by the system	yes	172800	172800
Starting port for resource manager services	Type a starting port number (the first of five consecutive numbers) to be used for resource manager components (migrator, purger, stager, replicator, and asynchronous recovery)[2]	yes	7500	7500
Enable LDAP	Select this check box to manage user IDs and passwords on an enterprise level.[3]	yes	cleared	No

Notes:
If you are using WebSphere Application Server Version 6.0, the default value is still the short name of the machine, but with `Node01` appended to it.
You can type a port number other than the recommended default number. However, it must be the first number of five available contiguous port numbers.

Table 10. Configuring the resource manager application ports

Field name	Description	Default name / option	Actual value here
HTTP port	The port number for the Web server that is configured for use with your application server	80	80
HTTPS port	The secure Web application port number that the system administration client uses to communicate with the resource manager application	443	443
Application server security enabled	Select this check box to indicate that you have previously enabled security for your application server.	cleared	yes
Secure Sockets Layer Option	Click **Use and configure IBM® HTTP Server SSL** for the install program to configure SSL for you. Click Use pre-configured settings for IBM HTTP Server SSL if you have already manually configured SSL and you want the resource manager Web application to use your settings. Click Do not use IBM HTTP Server SSL if you want WebSphere to be used as the SSL type. Type values for your ports that were assigned by WebSphere during deployment.	Use and configure IBM HTTP Server SSL	No

Table 11. Configuring Secure Sockets Layer

Field name	Description	Default name / option	Actual value here
Common name	The fully qualified name of the Web server where the resource manager application resides	Detected host name of the system	No
Organization	Your company name	IBM	No
Organizational Unit	Your organization section or department	DB2® Content Manager	No
Locality	Your city	SVL	No
State or province	Abbreviated name (2 characters)	CA	No
Country	Abbreviated name (2 characters)	US	No

Table 12. Defining location of system configuration files

Field name	Description	Default name / option	Actual value here
Select Local or Remote	Specify **Local** to install the system configuration files locally. Specify **Remote** to open another window where you specify the location of the system configuration files on a remote mapped drive, HTTP server, or LDAP server.	Local	/home/ibmcmadm/cmgmt/connectors

Table 13. Connecting system administration client to library server

Field name	Description	Field applies only if the library server was not selected along with the system administration client when you selected installation components	Default name / option	Actual value here
Database server type	Specify DB2 or Oracle as the database type for the library server.	yes	DB2	DB2

Library server database name	The name of your library server.		icmnlsdb	icmnlsdb
Library server schema name	Type the existing schema name for your library server.		icmadmin	icmadmin
Authentication type	Related to DB2 database authentication. Choose **Client** or **Server** to match the settings on your DB2 server.		Server	Server
Enable single sign-on for client authentication	Allows users to authenticate through their operating system			
Configure connection to remote library server database	Select to configure the system administration client to connect to a remote library server.	yes	cleared	yes
Enable LDAP for importing users	Select this check box to manage user IDs and passwords on an enterprise level.		cleared	yes

Table 14. System administration client connection to library server

Field name	Description	Default name / option	Actual value here
Library server connection ID	The shared database connection ID that is authorized to connect to the library server	icmconct	icmconct
Password	Type the password for the library server connection ID (do not copy and paste the password).		cmct83

Table 15. Remote connection to the library server database

Field name	Description	Default name / option	Actual value here
Library server operating system	The operating system where the library server is installed		AIX 6.1
Library server host name	The fully qualified host name of the machine where the library server resides.	Detected host name on your local machine (change it to the host name of the machine where the remote library server resides)	admsrv1
Library server database name	The name of the library server on the remote machine	icmnlsdb	icmnlsdb
Database port	The port number the system administration client uses to access the library server	50000	50000
Node name	The name of the machine where the library server resides	Detected short name of the local machine (change it to the short name of the machine where the remote library server resides)	admsrv1

Table 16. Library server connection to remote resource manager database

Field name	Description	Default name / option	Actual value here
Resource manager database server host name	The fully qualified host name of the machine where the resource manager database resides.	Detected host name on your local machine (change it to the host name of the machine where the remote resource manager database resides)	admsrv1
Resource manager operating system	The operating system where you installed the remote resource manager database		AIX 6.1
Resource manager database name	The name of the resource manager database that exists on the remote machine	rmdb	rmdb
Resource manager administration ID	The administration ID for the resource manager database on the remote machine.	rmadmin	rmadmin
Password	Type the password for the resource manager administration ID (do not copy and paste the password).	Password must match the password associated with the resource manager administration ID	cmrm83

Table 17. Library server connection to remote resource manager application

Field name	Description	Default name / option	Actual value here
Resource manager application host name	The fully qualified host name of the machine where the resource manager Web application resides.	detected host name on your local machine (change it to the host name of the machine where the remote resource manager application resides)	admsrv1
Web application name	The name of the Web application that is deployed on your application server.	icmrm	icmrm
Resource manager Web application context root	The context root of the resource manager application that is used to construct the Web address of the resource manager Web application.	/icmrm	/icmrm
Resource manager Web application port	The port number used to access the resource manager application.	80	80
Resource manager secure Web application port	The port number that the system administration client uses to communicate with the resource manager application	443	443

Important: If you are using DB2 UDB, you must catalog the library server database on the machine where the resource manager application resides for a remote library server and resource manager application to communicate. If you are using Oracle, you must add the library server database entry in `tnsnames.ora` on the machine where the resource manager application resides.

Table 18. Resource manager database connection to remote library server database

Field name	Description	Default name / option	Actual value here
Library server host name	The fully qualified host name of the machine where the library server database resides.	Detected host name on your local machine (change it to the host name of the machine where the remote library server database resides)	admsrv1
Library server operating system	The operating system where you installed the remote library server database		AIX 6.1
Library server database name	The name of the library server database that exists on the remote machine	icmnlsdb	icmnlsdb
Library server schema name	The schema name of the library server database on the remote machine that is used to group tables and other objects.	icmadmin	icmadmin
Library server administration ID	The administration ID for the library server database on the remote machine.	icmadmin	icmadmin
Password	Type the password for the library server administration ID (do not copy and paste the password).	Password must match the password associated with the library server administration ID	passwd

Table 19. Resource manager database connection to remote resource manager application

Field name	Description	Default name / option	Actual value here
Resource manager application host name	Type the fully qualified host name of the machine where the resource manager application is located.		admsrv1
Resource manager Web application name	The name of the Web application that is deployed on your application server.	icmrm	icmrm
Resource manager Web application context root	The context root that is used to construct the Web address of the resource manager Web application.	/icmrm	/icmrm
Resource manager Web application port	The port number used to access the resource manager application.	80	80
Resource manager secure Web application port	The port number that the system administration client uses to communicate with the resource manager application.	443	443
Token duration (seconds)	The amount of time in seconds that a token generated by the library server for a particular operation on the resource manager is active before it is discarded by the system.	172800	172800

Table 20. Resource manager application connection to remote resource manager database

Field name	Description	Default name / option	Actual value here
Resource manager database server host name	The fully qualified host name of the machine where the resource manager database resides.	Detected host name on your local machine (change it to the host name of the machine where the remote resource manager database resides).	admsrv1
Resource manager operating system	The operating system where you installed the remote resource manager database.		AIX 6.1
Resource manager database server type	The server type for the resource manager database.		DB2
Resource manager database name	The name of the resource manager database that exists on the remote machine.	rmdb	rmdb

Important: If you are using DB2 UDB, you must catalog the resource manager database on the machine where the resource manager application resides.

Table 21. Resource manager database authentication information

Field name	Description	Default name / option	Actual value here
Resource manager administration ID	The administration ID for the resource manager database on the remote machine.	rmadmin	rmadmin
Password	Type the password for the resource manager administration ID (do not copy and paste the password).	Password must match the password associated with the resource manager administration ID	cmrm83

Table 22. Defining the LDAP server

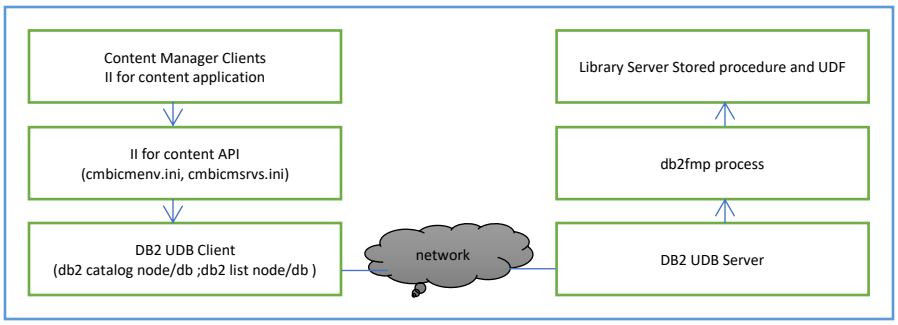
Field name	Description	Default name / option	Actual value here
LDAP server type	Select either **Standard LDAP**[1] or **Active Directory** from the list.	Standard LDAP	No
LDAP server address (URL)	The address for your LDAP server	ldap:// ldapserver.ibm.com	No
Port	The port number of the LDAP server	389	No
LDAP server administration ID	The administration ID that already exists for your LDAP server		No
Password	Type the existing password for the LDAP server administration ID[2]		No

Notes:
Select Standard LDAP if you are using a supported version of IBM® Directory Server, Tivoli® Directory server, or Lotus® Domino® Directory, or Sun Java™ System Directory Server.
Type the password. Do not copy and paste it.

DB2 Content Manager Software Installation directory

AIX/Linux: /opt/IBM/db2cmv8
Windows: C:\Program Files\IBM\db2cmv8\

pClient connection setting (to Library server) on PC

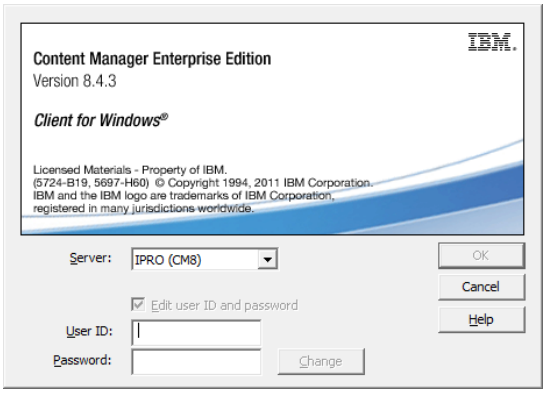


By default, DB2 Content Manager logon processing will first attempt to authenticate the user ID through DB2 Universal Database™. If it is successful, it will not check the password stored in the DB2 Content Manager library server ICMSTUSERS table. If DB2 authentication fails, DB2 Content Manager logon processing would then use the encrypted user ID/password pair stored in **cmbicmenv.ini** (Example, ICMCONCT) to authenticate with DB2 Universal Database. Assuming the ICMCONCT user ID/password authenticates successfully to DB2 Universal Database, only then would DB2 Content Manager logon processing proceed to check the given user ID/password (passed in by the user at logon) against the corresponding user ID/password in the DB2 Content Manager library server ICMSTUSERS table.

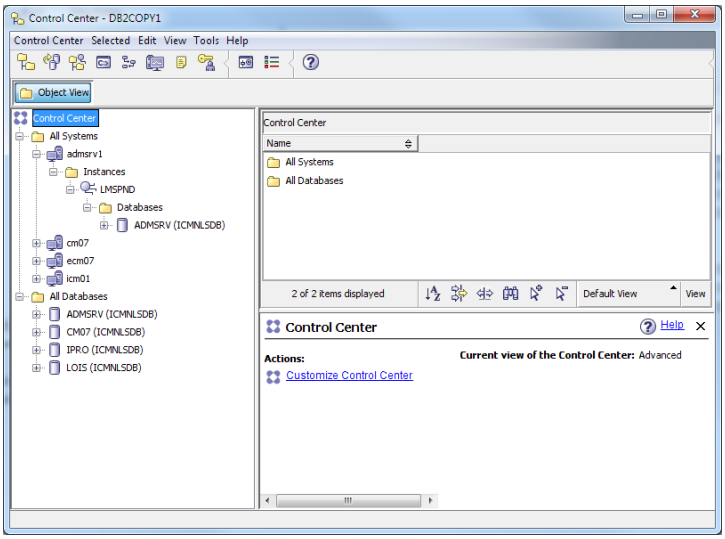
installation

if you have old pClient and DB2 UDB Client software installed, delete them clearly, especially delete them from register key(regedit)

1. unzip and install winClient8.4.03.400 package(setup), this is pclient software



2. unzip and install v97fp11_nt32_client.exe, this is DB2 UDB client software,



Update pClient connection setting C:\Program Files\IBM\db2cmv8\cmgmt\connectors**cmbicmsrvs.ini**

ICMSERVER=cm07
ICMSERVERREPTYPE=DB2
ICMSCHEMA=icmadmin
ICMSSO=FALSE
ICMDBAUTH=SERVER
ICMREMOTE=TRUE
ICMHOSTNAME=cm07
ICMPORT=50000
ICMREMOTEDB=icmnlsdb
ICMNODENAME=lmsdnd
ICMOSTYPE=AIX

```
ICMSERVER=admsrv
ICMSERVERREPTYPE=DB2
ICMSCHEMA=icmadmin
ICMSSO=FALSE
ICMDBAUTH=SERVER
ICMREMOTE=TRUE
ICMHOSTNAME=admsrv1
ICMPORT=50000
ICMREMOTEDB=icmnlsdb
ICMNODENAME=lmspnd
ICMOSTYPE=AIX

ICMSERVER=LOIS
ICMSERVERREPTYPE=DB2
ICMSCHEMA=icmadmin
ICMSSO=FALSE
ICMDBAUTH=SERVER
ICMREMOTE=TRUE
ICMHOSTNAME=icm01
ICMPORT=50000
ICMREMOTEDB=icmnlsdb
ICMNODENAME=loispnd
ICMOSTYPE=AIX

ICMSERVER=IPRO
ICMSERVERREPTYPE=DB2
ICMSCHEMA=icmadmin
ICMSSO=FALSE
ICMDBAUTH=SERVER
ICMREMOTE=TRUE
ICMHOSTNAME=ecm07
ICMPORT=50000
ICMREMOTEDB=icmnlsdb
ICMNODENAME=ipropnd
ICMOSTYPE=AIX
```

when you login CM Library server, pClient will update DB2 UDB client software automatically with these configuration!

```
C:\Program Files\IBM\SQLLIB\BIN>db2 list node directory

 Node Directory

 Number of entries in the directory = 4

Node 1 entry:

 Node name                      = IPROPND
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = TCPIP
 Hostname                       = ecm07
 Service name                   = 50000

Node 2 entry:

 Node name                      = LMSDND
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = TCPIP
 Hostname                       = cm07
```

Service name = 50000

Node 3 entry:

Node name = LMSPND
Comment =
Directory entry type = LOCAL
Protocol = TCPIP
Hostname = admsrv1
Service name = 50000

Node 4 entry:

Node name = LOISPND
Comment =
Directory entry type = LOCAL
Protocol = TCPIP
Hostname = icm01
Service name = 50000

C:\Program Files\IBM\SQLLIB\BIN>db2 list db directory

System Database Directory

Number of entries in the directory = 4

Database 1 entry:

Database alias = LOIS
Database name = ICMNLSDB
Node name = LOISPND
Database release level = d.00
Comment =
Directory entry type = Remote
Authentication = SERVER
Catalog database partition number = -1
Alternate server hostname =
Alternate server port number =

Database 2 entry:

Database alias = ADMSRV
Database name = ICMNLSDB
Node name = LMSPND
Database release level = d.00
Comment =
Directory entry type = Remote
Authentication = SERVER
Catalog database partition number = -1
Alternate server hostname =
Alternate server port number =

Database 3 entry:

Database alias = IPRO
Database name = ICMNLSDB
Node name = IPROPND
Database release level = d.00
Comment =

Directory entry type = Remote
Authentication = SERVER
Catalog database partition number = -1
Alternate server hostname =
Alternate server port number =

Database 4 entry:

Database alias = CM07
Database name = ICMNLSDB
Node name = LMSDND
Database release level = d.00
Comment =
Directory entry type = Remote
Authentication = SERVER
Catalog database partition number = -1
Alternate server hostname =
Alternate server port number =

Database connection parameter file

on PC, to setup pClient connection, batch file to setup ICMCONCT authentication in **cmbicmenv.ini**

```
-a <add>  (action)
   -s <library server database name>
   -u <database userid>
   -p <database password>
   -d  <directory path location cmbicmenv.ini> (default current directory)
```

U:\> set PATH=C:\Program Files\IBM\db2cmv8\java\jre\bin;%PATH%
U:\> set CLASSPATH=C:\Program Files\IBM\db2cmv8\lib\cmbutil81.jar;C:\Program Files\IBM\db2cmv8\lib\cmbutilicm81.jar;.;%CLASSPATH%
U:\> java com.ibm.mm.sdk.util.cmbenvicm -a add -s **lmsdevls** -u icmconct -p cmctev

U:\> more cmbicmenv.ini
lmsdevls=(aWNtY29uY3Q7Y21jdGRldg==)

C:\Program Files\IBM\db2cmv8\cmgmt\connectors**cmbicmenv.ini**
lmsdevls=(aWNtY29uY3Q7Y21jdGRldg==)
VMLS=(aWNtY29uY3Q7aWNtY29uY3Q=)

If you know that your users are all Content Manager internal user IDs or LDAP user IDs (and have no DB2 connection privileges), you can change ICMSERVERREPTYPE to DB2CON. This avoids the first step mentioned above, and goes directly to cmbicmenv.ini, and connects to the Library Server database using the user ID and password in the cmbicmenv.ini file, then calls ICMLOGON. It improves the performance of the entire logon process, too. Note that you can modify this behavior by changing ICMSERVERREPTYPE from DB2 to DB2CON in your cmbicmsrvs.ini. ICMSERVERREPTYPE=DB2CON effectively reverses the order of the user IDs used for authentication during DB2 Content Manager logon processing. With DB2CON, the user ID/password pair in cmbicmenv.ini (for example, the "ICMCONCT" user ID) is checked first for authentication to DB2 Universal Database and if it authenticates successfully then the given user ID/password (passed in from the user logon) will be checked against the corresponding user ID/password value stored in the library server ICMSTUSERS table and no attempt will be made to authenticate with DB2 Universal Database using that given user ID/password (passed in from the user logon). If the ICMCONCT authentication fails, the given user ID/password (passed in from the user logon) is used during DB2 Content Manager logon processing to attempt to authenticate with DB2 Universal Database.

The previous discussion assumes a user ID for which the **Use system password** check box in the System Administration Client Define Users window is **not selected**. It also assumes that the library server logon user exit is not in effect. If the **Use system password** check box were selected for the user ID and the library server logon user exit were not in effect, then authentication

would succeed only by authenticating to DB2 Universal Database using the given user ID/password and not the user ID/password pair stored in the cmbicmenv.ini file. In this scenario the given user ID would need DB2 authority. The library server logon user exit is required to authenticate to DB2 Universal Database by using the user ID/password pair stored in the cmbicmenv.ini file in conjunction with a given user ID/password for which the **Use system password** check box is selected. In this scenario the given user ID would not need DB2 authority

For DB2 UDB connection slow problem, we found that if we cataloged the Library Server database using **AUTHENTICATION SERVER** on the client machine, the ICMCONCT connected to Library Server database as fast as any other operating system user IDs, meaning that the entire Content Manager logon performance issue was gone. For example

```
UNCATALOG DATABASE VMLS;
CATALOG DATABASE ICMNLSDB AS VMLS AT NODE VMIN1 AUTHENTICATION SERVER;
```

System administration client(on Linux)

The system administration client provides the tools that you need to set up and manage your system. The system administration client provides the tools that you need to set up and manage your Content Manager system. When you work with the system administration client (such as create, change, and remove an item type; create and remove a user ID)

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 connecting 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.

Database connection parameter file:

- IBM Content Manager: cmbicmsrvs.ini;
- IBM Information Integrator for Content: cmbds.ini

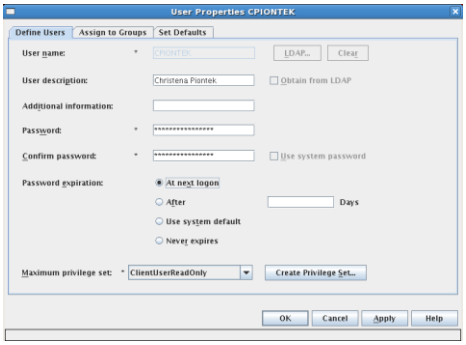
The database connection parameter file stores the connection parameters that the system administration client needs to connect to the remote database. The following list defines each parameter in the **cmbicmsrvs.ini** file, the file that defines the connection parameters between the IBM Content Manager system administration client and the library server.

Location of DB2 <Content Manager System administration client> system configuration files on Liru Chen's Laptop: /home/ibmcmadm/cmgmt/connectors

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.

```
[root@ibmserver connectors]# more cmbicmsrvs.ini
ICMSERVER=ibmserver(icmnlsdb)
ICMSERVERREPTYPE=DB2
ICMSCHEMA=icmadmin
ICMSSO=FALSE
ICMDBAUTH=SERVER
ICMREMOTE=TRUE
ICMHOSTNAME=ibmserver
ICMPORT=50000
ICMREMOTEDB=icmnlsdb
ICMNODENAME=
ICMOSTYPE=LINUX
ICMJDBCDRIVER=
ICMJDBCURL=
ICMJNDIREF=
ICMDBVER=
ICMGMTSYSATTRTS=

ICMSERVER=CM07(icmnlsdb)
ICMSERVERREPTYPE=DB2
ICMSCHEMA=icmadmin
ICMSSO=FALSE
ICMDBAUTH=SERVER
ICMREMOTE=TRUE
ICMHOSTNAME=cm07
ICMPORT=50000
ICMREMOTEDB=icmnlsdb
ICMNODENAME=TEST
ICMOSTYPE=AIX
ICMJDBCDRIVER=
ICMJDBCURL=
ICMJNDIREF=
ICMDBVER=
ICMGMTSYSATTRTS=

ICMSERVER=LMS(icmnlsdb)
ICMSERVERREPTYPE=DB2
ICMSCHEMA=icmadmin
ICMSSO=FALSE
ICMDBAUTH=SERVER
ICMREMOTE=TRUE
ICMHOSTNAME=admsrv1_svc
ICMPORT=50000
ICMREMOTEDB=icmnlsdb
ICMNODENAME=
ICMOSTYPE=AIX
ICMJDBCDRIVER=
ICMJDBCURL=
ICMJNDIREF=
ICMDBVER=
ICMGMTSYSATTRTS=
```



Starting the Content Manager System administration client

xhost +

(modify the xhost settings to allow remote servers to log on to your server)

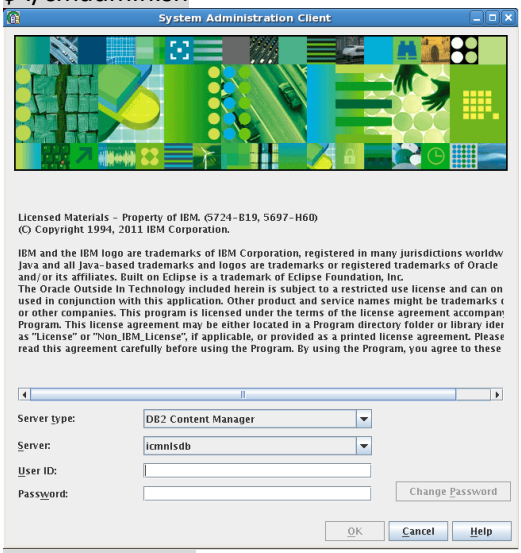
TIPS: Run System Administration Client on your windows laptop,

1. install Xserver (eg. Xming) on your laptop, and start X Server
2. On CM Server, Config /etc/ssh/sshd_config, set X11FORWORDING yes, and restart sshd services
3. login CM server using ssh client with X11 forwaording enabled

su – icmadmin

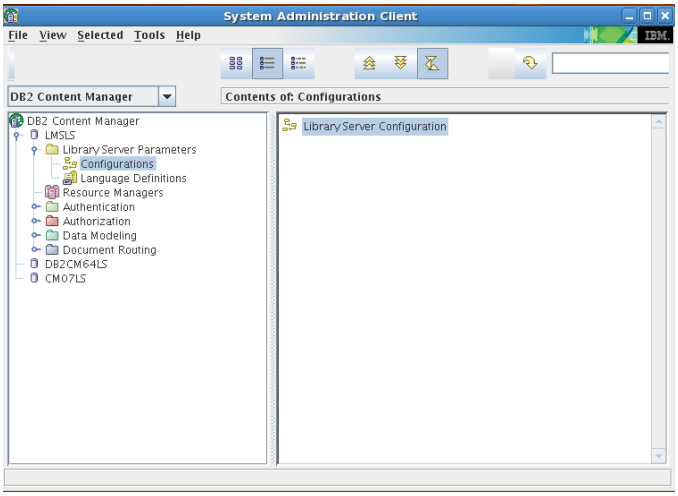
$ cd /opt/IBM/db2cmv8/admin/common

$ ./cmadmin.sh



User ID: icmadmin

Password: passwd

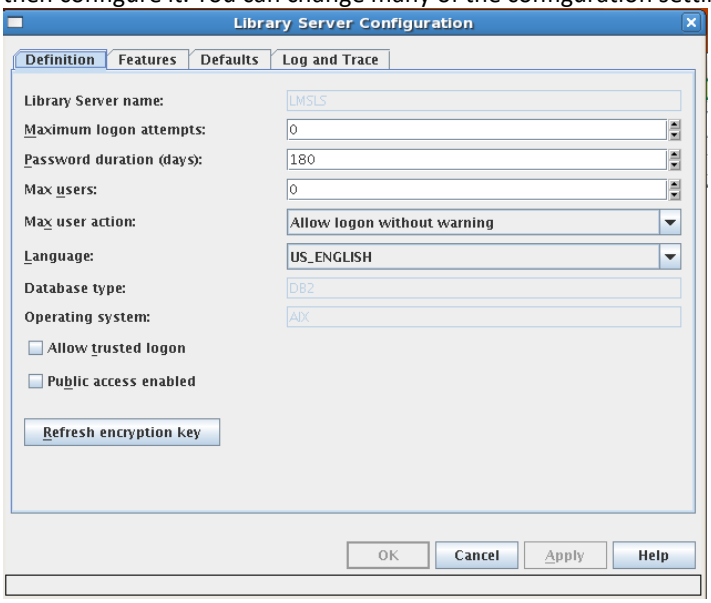


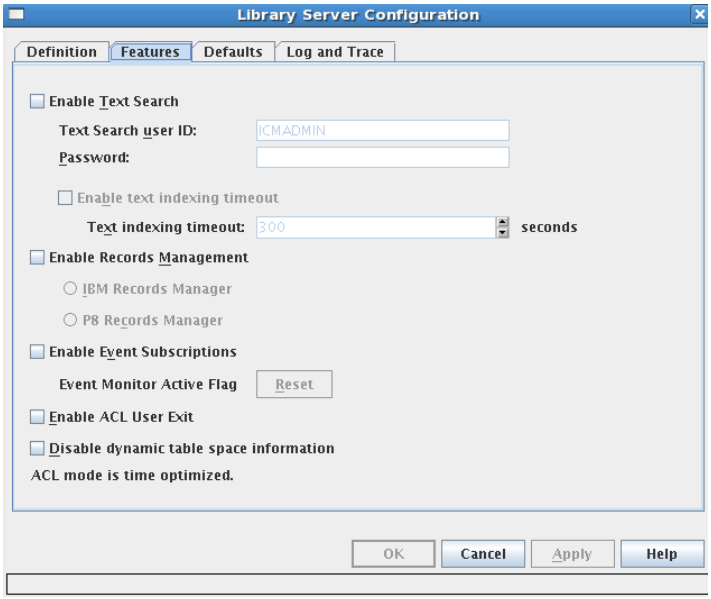
TIPS: Administration ID must exist on your operating system, You should create a User ID in OS if you need to create a new administration account in DB2 content manager, the User ID (name) should be the same in OS and CM

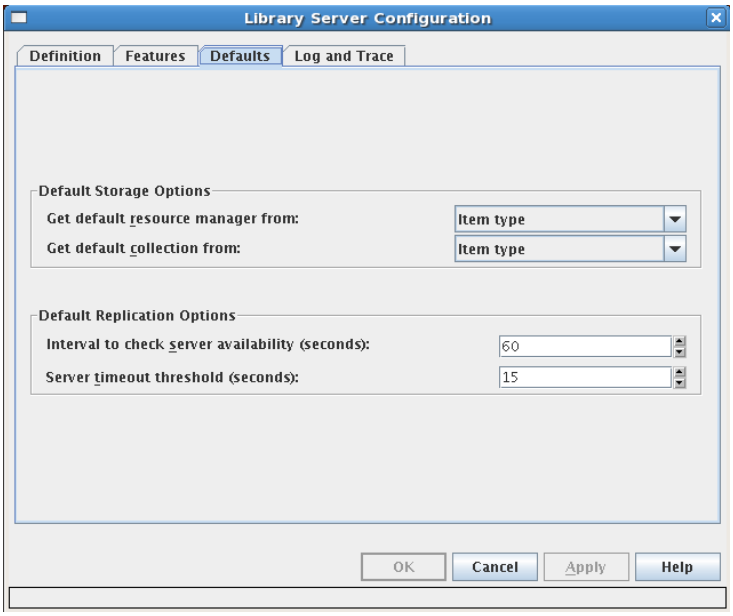
Library server

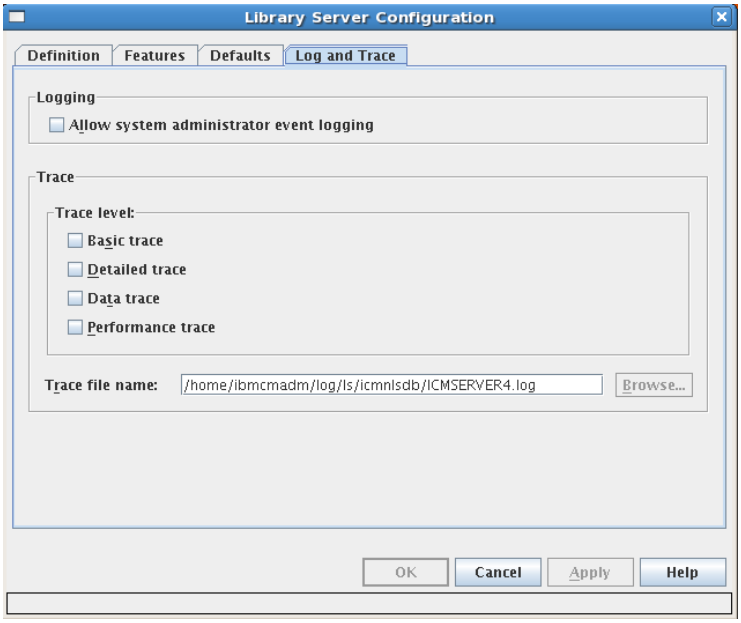
The key component of IBM Content Manager, stores, manages, and provides access control for objects stored on one or more resource managers.

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.




Library Server Configuration
Definition
Features
Defaults
Log and Trace
Enable Text Search
Text Search user ID:
ICMADMIN
Password:
Enable text indexing timeout
Text indexing timeout:
300
seconds
Enable Records Management
IBM Records Manager
P8 Records Manager
Enable Event Subscriptions
Event Monitor Active Flag
Reset
Enable ACL User Exit
Disable dynamic table space information
ACL mode is time optimized.
OK
Cancel
Apply
Help


Library Server Configuration
Definition
Features
Defaults
Log and Trace
Default Storage Options
Get default resource manager from:
Item type
Get default collection from:
Item type
Default Replication Options
Interval to check server availability (seconds):
60
Server timeout threshold (seconds):
15
OK
Cancel
Apply
Help



You can enable the logging and tracing for the all of CM components or services

Resource manager

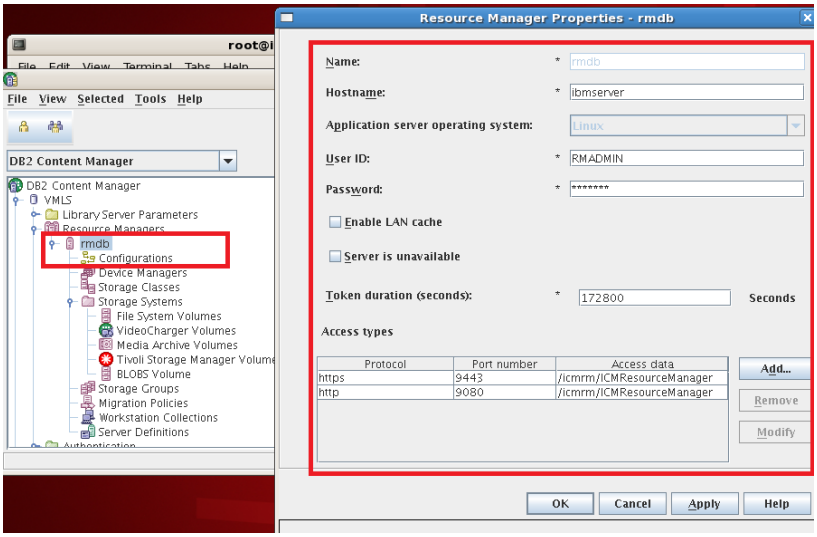
The resource manager is the repository for content stored in the IBM Content Manager system. Objects are stored in the resource manager, and the associated attribute data is stored on the library server. Resource manager manages object storage consists of creating the collections that organize the objects in your system and creating the additional entities that support the collections.

$ cd /usr/IBM/WebSphere/AppServer/profiles/AppSrv02/bin

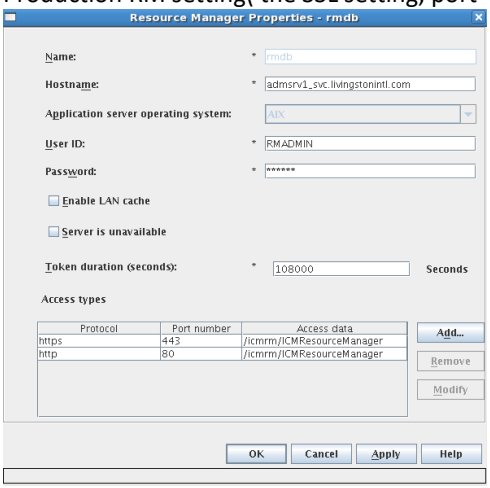
To check the status of the resource manager application server, enter:
$ ./serverStatus.sh icmrm

To start the resource manager application server, enter the following commands, each on a separate line:
$. /home/db2inst1/sqllib/db2profile
$ ./startServer.sh icmrm

To stop the resource manager application server, enter:
$ ./stopServer.sh icmrm



Production RM setting(the SSL setting, port 443, is NOT working)



The 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:

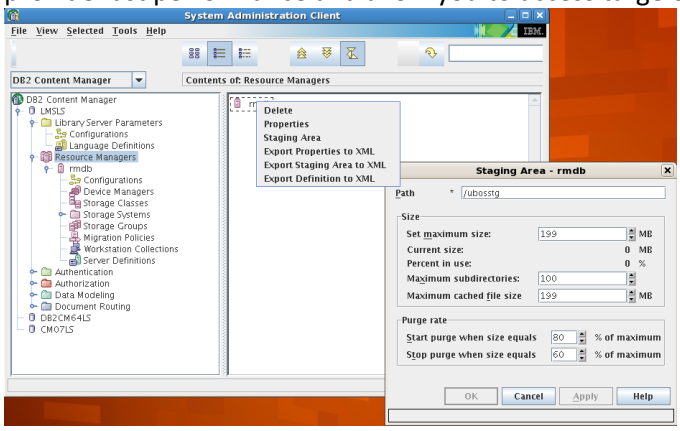
1. Deploy the resource manager in WebSphere Business Integration Server Foundation or WebSphere Application Server. See Planning and Installing Your Content Management System for information about deploying a resource manager. Make note of the following information about the new resource manager:
   - 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.

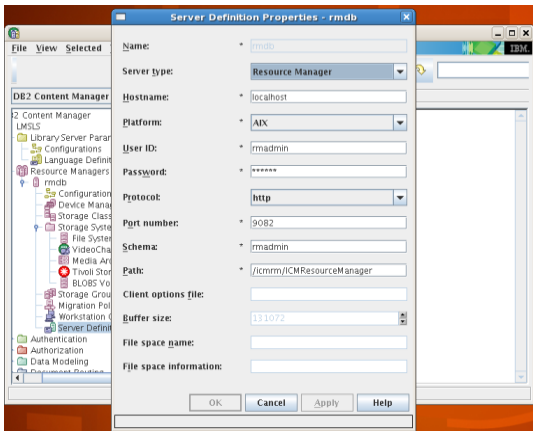
4. Define the new resource manager in the library server:
5. Optional: If you enabled **LAN cache** or plan to use IBM **Tivoli® Storage Manager**, modify **the staging area** properties to meet your needs.

   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 targe objects that could be stored on slower devices.



6. Configure the resource manager.
7. Set up server definitions among all existing resource managers.

   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.



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.

Access type: 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

If those values do not work, check the HTTP transport settings in WebSphere Application Server
/usr/IBM/HTTPServer/bin/adminctl start|stop

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.

View the snoop information provided by the resource manager for a regular connection. Enter the appropriate URL in the browser.
http://admsrv1/icmrm/snoop
http://admsrv1:9082/icmrm/snoop

Important: The admin.conf configuration file supports single-byte characters (SBCS) only.
Confirm that IBM HTTP Server administration server started successfully by checking the admin_error.log file.

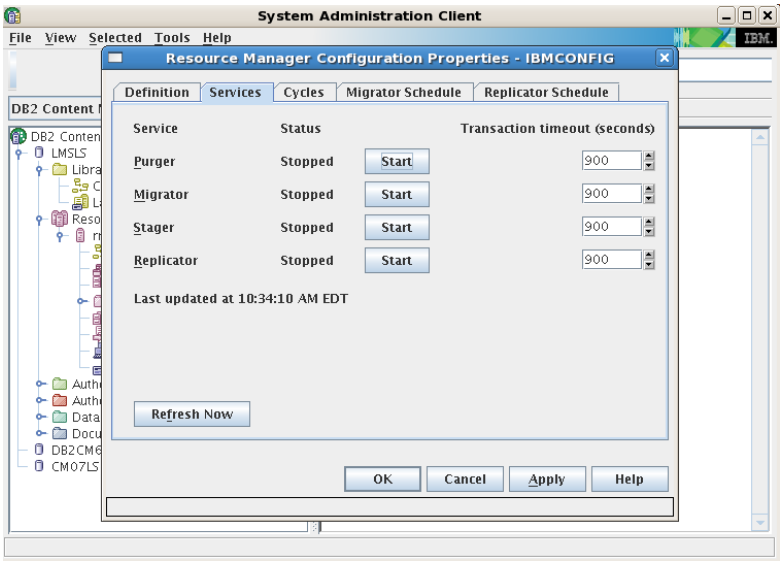
Tip: The port number is typically 9081 for HTTP connections and 9444 for HTTPS connections

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 MTRANSACTIONS 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.

Four resource manager services



- Purger: If LAN cache is enabled or if Tivoli Storage Manager is in use to maintain the size of the staging area. When the staging area size reaches a preset upper limit, the purger will begin to remove files until it reaches a preset lower limit
- Migrator Always; 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.
- Stager: If DB2 Content Manager VideoCharger or another media archiver is in use
- Replicator: If replicas are defined; 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.

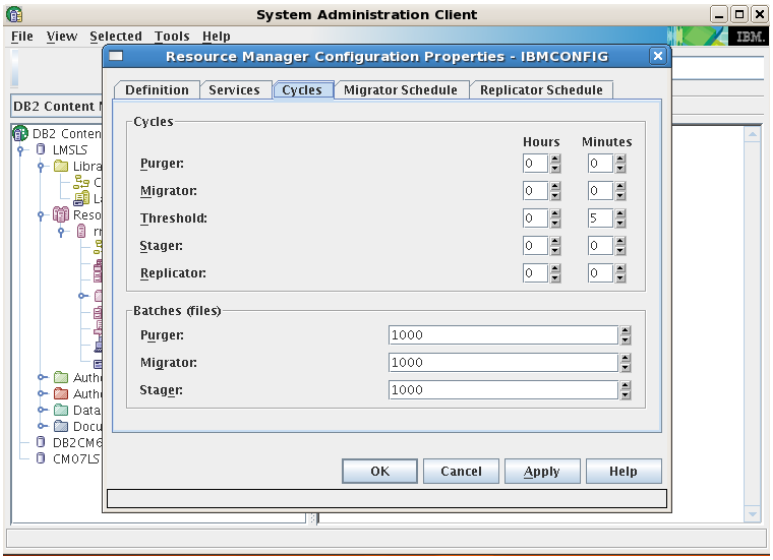
To start all four applications:
/etc/rc.cmrmprc -act start -db <dbname> -app <rmappname>

To stop all four applications:
/etc/rc.cmrmproc -act stop -db <dbname> -app <rmappname>

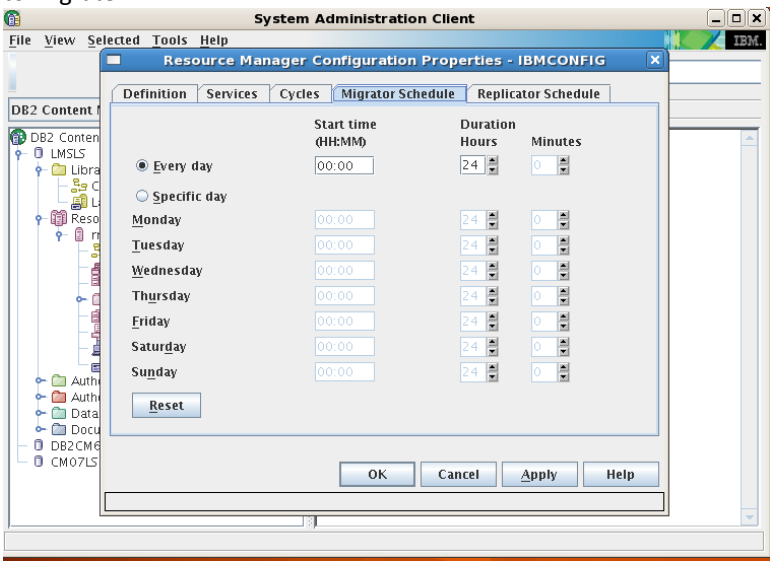
To start select applications:
/etc/rc.cmrmproc -act start -db <dbname> -app <rmappname> -proc <application>
<application> is the Resource Manager stand-alone process you want to start. For example, to start Resource Manager migrator, RMMigrator, on database rmdb with icmrm as the Resource Manager Web application, use:
/etc/rc.cmrmproc -act start -db rmdb -app icmrm -proc RMMigrator

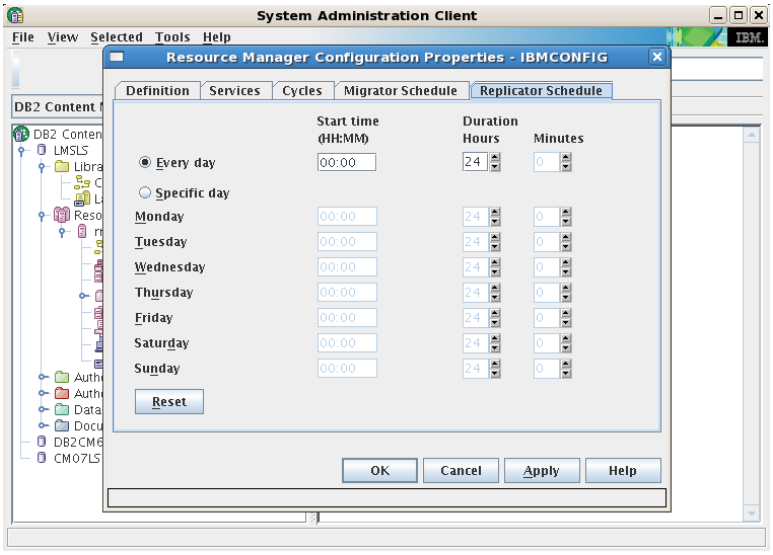
To stop select applications:
/etc/rc.cmrmproc -act stop -db <dbname> -app <rmappname> -proc <application>

To start all four applications using the default values for dbname and rmappname, specified in the $IBMCMROOT/config/setprocenv.sh file: /etc/rc.cmrmproc start



Type or select the amount of time in hours and minutes that must elapse before the purger begins purging if necessary;
Type or select the amount of time in hours and minutes that must elapse before the migrator checks if there is anything to migrate





When the migrator starts periodically, it runs queries against the Resource Manager database to find a batch of documents that are based on obj_actiondate and volume information in the RMOBJECTS table. It then migrates these documents to the next point in the migration path. In most cases, they go from a physical disk (where they start when they first arrive) to Tivoli Storage Manager. When a document is migrated from hard disk to TSM, the RMOBJECTS table is updated so that the document's obj_actiondate is changed and its obj_volumeid is changed to the volumeid for the proper TSM Management class.

Important: Remember to have the Content Manager migrator process running at all times, even if you do not migrate objects between storage classes, because it is used to physically delete objects from where the Resource Manager has stored them. When a user deletes an object from the standard client, only the row from the Library Server database is deleted immediately (for performance reasons), and the entry in the Resource Manager database and the object itself remain. The migrator must be run to reclaim the physical storage space.

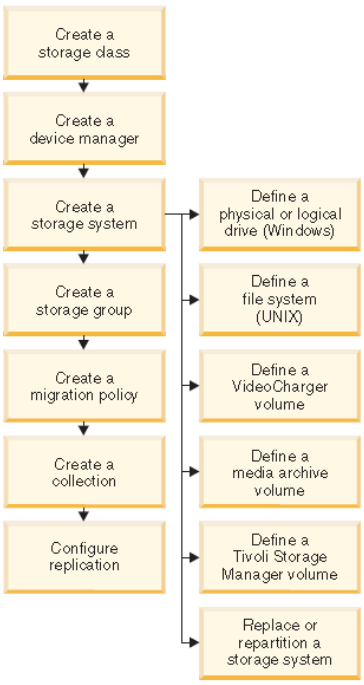
Managing object storage

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:

   Define a physical or logical drive (Windows)
   Define a file system (UNIX) -- LMS
   Define a VideoCharger
   volume Define a media archive volume
   Define a Tivoli Storage Manager volume
   Replace or repartition a storage system

4. Create a storage group
5. Configure migration.
6. Create a collection.
7. Configure replication.



On LMS Produciton, Define a file systems and assign them to a defined storage group

Create HACMP Concurrent Volume Group On admsrv1
#smitty hacmp - > System Management - > Storage - > Volume Groups - > Create a Volume Group
Choose Node Names (admsrv1, admsrv2) by press F7

- Creat enhanced concurent mode Volume Group (Create VG Concurrent Capable? Yes)
- Add shared volume groups to HACMP resource group
- Create file systems

Add hdisk40, hdisk41 and hdisk42 to Volume Group: docvg4 with:

Volume Group major number:	107
Active volume group automatically at system restart:	no
Create VG Concurrent Capable?	enhanced concurrent

$ lsvg doc4vg

```
VOLUME GROUP:       admsrv1_doc4vg          VG IDENTIFIER:  00f86f6200004c0000000143a7cecf2c
VG STATE:           active                  PP SIZE:        256 megabyte(s)
VG PERMISSION:      read/write              TOTAL PPs:      1596 (408576 megabytes)
MAX LVs:            256                     FREE PPs:       396 (101376 megabytes)
LVs:                3                       USED PPs:       1200 (307200 megabytes)
OPEN LVs:           3                       QUORUM:         1 (Disabled)
TOTAL PVs:          4                       VG DESCRIPTORS: 4
STALE PVs:          0                       STALE PPs:      0
ACTIVE PVs:         4                       AUTO ON:        no
Concurrent:         Enhanced-Capable        Auto-Concurrent: Disabled
VG Mode:            Concurrent
Node ID:            2                       Active Nodes:
MAX PPs per VG:     32512
MAX PPs per PV:     1016                    MAX PVs:        32
LTG size (Dynamic): 256 kilobyte(s)         AUTO SYNC:      no
HOT SPARE:          no                      BB POLICY:      relocatable
PV RESTRICTION:     none                    INFINITE RETRY: no
```

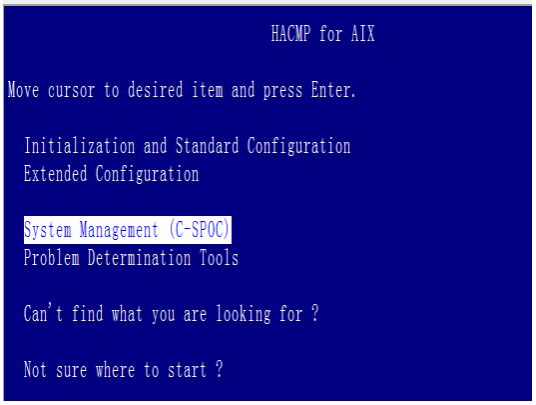
On admsrv2:
$ lsvg doc4vg

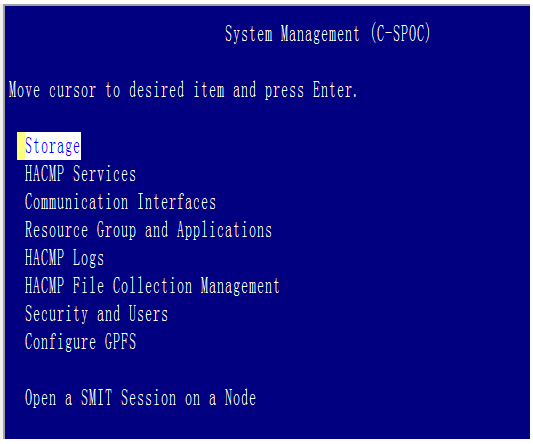
```
VOLUME GROUP:       admsrv1_doc4vg          VG IDENTIFIER:  00f86f6200004c0000000143a7cecf2c
```

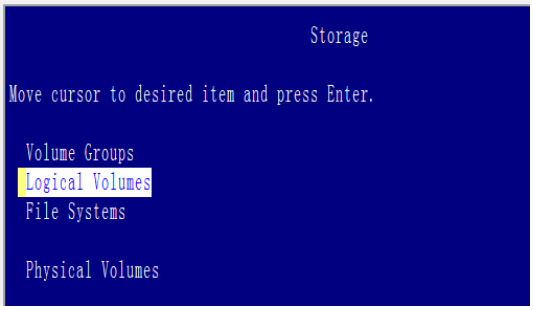
```
VG STATE:           active                   PP SIZE:        256 megabyte(s)
VG PERMISSION:      passive-only             TOTAL PPs:      1596 (408576 megabytes)
MAX LVs:            256                      FREE PPs:       396 (101376 megabytes)
LVs:                3                        USED PPs:       1200 (307200 megabytes)
OPEN LVs:           0                        QUORUM:         1 (Disabled)
TOTAL PVs:          4                        VG DESCRIPTORS: 4
STALE PVs:          0                        STALE PPs:      0
ACTIVE PVs:         4                        AUTO ON:        no
Concurrent:         Enhanced-Capable         Auto-Concurrent: Disabled
VG Mode:            Concurrent
Node ID:            3                        Active Nodes:
MAX PPs per VG:     32512
MAX PPs per PV:     1016                     MAX PVs:        32
LTG size (Dynamic): 256 kilobyte(s)          AUTO SYNC:      no
HOT SPARE:          no                       BB POLICY:      relocatable
PV RESTRICTION:     none                     INFINITE RETRY: no
```

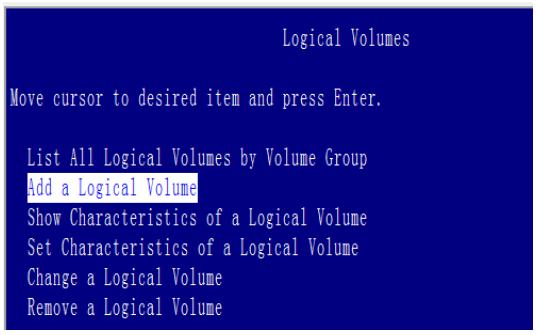
Create HACMP File Systems On admsrv1

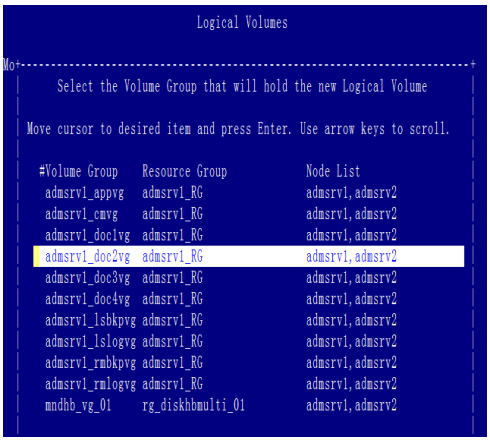
#smitty hacmp - > System Management - > Storage - > Volume Groups - > Create a Volume Group

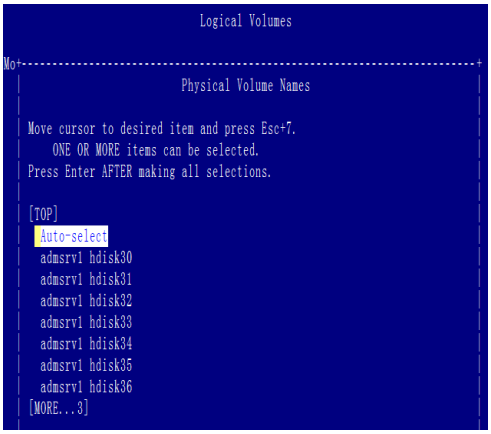


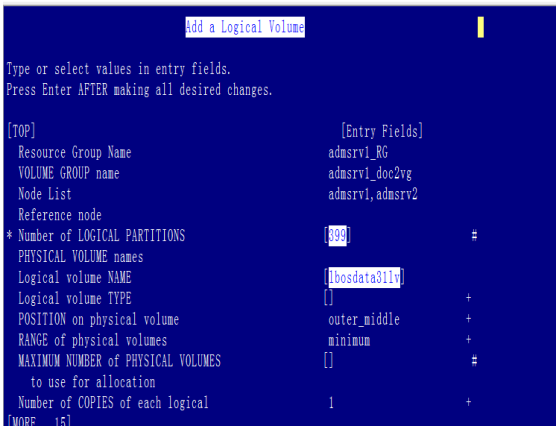


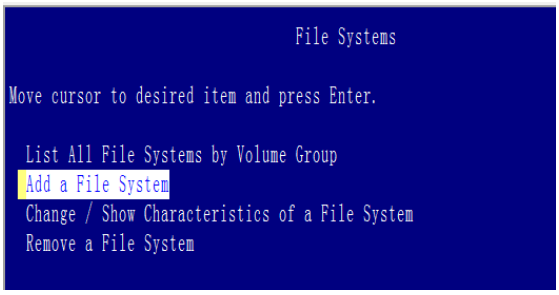



Logical Volumes
Move cursor to desired item and press Enter.
List All Logical Volumes by Volume Group
Add a Logical Volume
Show Characteristics of a Logical Volume
Set Characteristics of a Logical Volume
Change a Logical Volume
Remove a Logical Volume


Logical Volumes
Select the Volume Group that will hold the new Logical Volume
Move cursor to desired item and press Enter. Use arrow keys to scroll.
#Volume Group Resource Group Node List
admsrv1_appvg admsrv1_RG admsrv1,admsrv2
admsrv1_cmvg admsrv1_RG admsrv1,admsrv2
admsrv1_doc1vg admsrv1_RG admsrv1,admsrv2
admsrv1_doc2vg admsrv1_RG admsrv1,admsrv2
admsrv1_doc3vg admsrv1_RG admsrv1,admsrv2
admsrv1_doc4vg admsrv1_RG admsrv1,admsrv2
admsrv1_lsbkpvg admsrv1_RG admsrv1,admsrv2
admsrv1_lslogvg admsrv1_RG admsrv1,admsrv2
admsrv1_rmbkpvg admsrv1_RG admsrv1,admsrv2
admsrv1_rmlogvg admsrv1_RG admsrv1,admsrv2
mndhb_vg_01 rg_diskhbmulti_01 admsrv1,admsrv2


Logical Volumes
Physical Volume Names
Move cursor to desired item and press Esc+7.
ONE OR MORE items can be selected.
Press Enter AFTER making all selections.
[TOP]
Auto-select
admsrv1 hdisk30
admsrv1 hdisk31
admsrv1 hdisk32
admsrv1 hdisk33
admsrv1 hdisk34
admsrv1 hdisk35
admsrv1 hdisk36
[MORE...3]


Add a Logical Volume
Type or select values in entry fields.
Press Enter AFTER making all desired changes.
[TOP] [Entry Fields]
Resource Group Name admsrv1_RG
VOLUME GROUP name admsrv1_doc2vg
Node List admsrv1,admsrv2
Reference node
* Number of LOGICAL PARTITIONS [999] #
PHYSICAL VOLUME names
Logical volume NAME [lbosdata31lv]
Logical volume TYPE [] +
POSITION on physical volume outer_middle +
RANGE of physical volumes minimum +
MAXIMUM NUMBER of PHYSICAL VOLUMES [] #
to use for allocation
Number of COPIES of each logical 1 +
[MORE...15]



Expand **Resource Managers** in the tree view of System Administration Client.

Expand the resource manager that you want to work with.

Expand **Storage Systems**.

Right-click **File System Volumes** and click **New** to open the New File System Volume window.

In the **Device** field, select a device from the list. The device is the physical disk of your machine.

In the **Mount point** field, type a mount point for the volume. A mount point is a logical unit of a device.

Optional: In the **Default path** field, enter the path on the volume where the resource manager should store the data.

In the **Maximum subdirectories** field, type a 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.

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.

In the **Storage class** field, select a storageclass 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.

In the **Assignment** field, click a radio button to assign a relationship between the DB2® Content Manager volume and one or more storage groups.

Unassigned to prevent storage groups from using this volume as storage.

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.

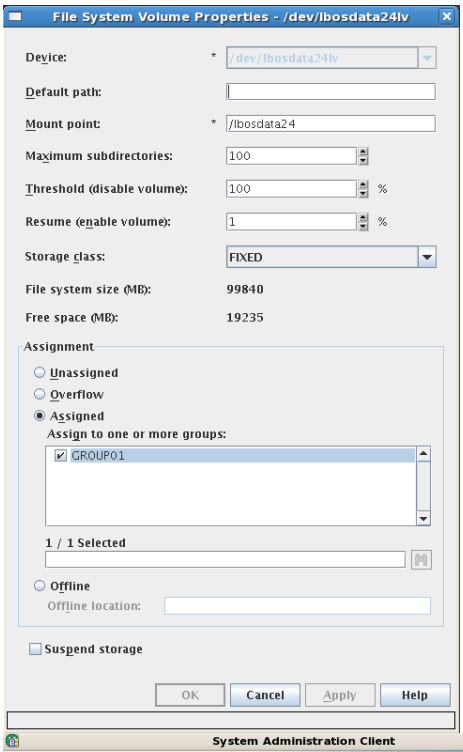
Assigned to associate the volume to the storage groups that you select in the **Assign one or more storagegroups** list.

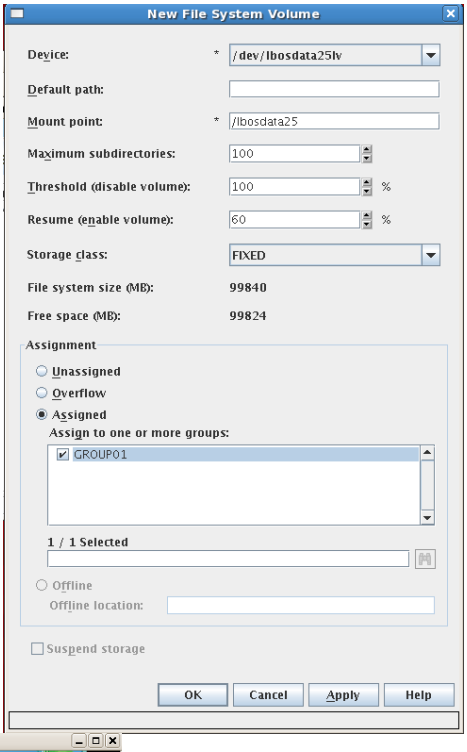
Selecting **Assigned** enables the **Suspend Storage** check box.

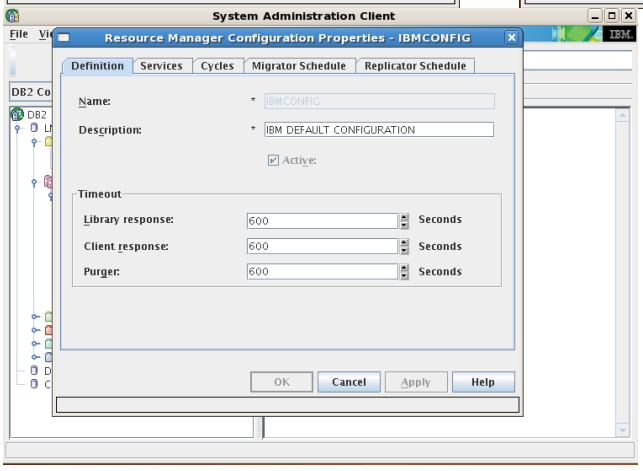
Suspendstorage to prevent resource managers from using a volume for new objects. If the volume is full, this check box is selected automatically.

Offline to indicate that the volume has been removed. **Optional:** In the **Offline location** field, indicate the location of the volume.

Click **OK** to save the volume







Managing User Access

For full administrative privileges to DB2 ,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.

- 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

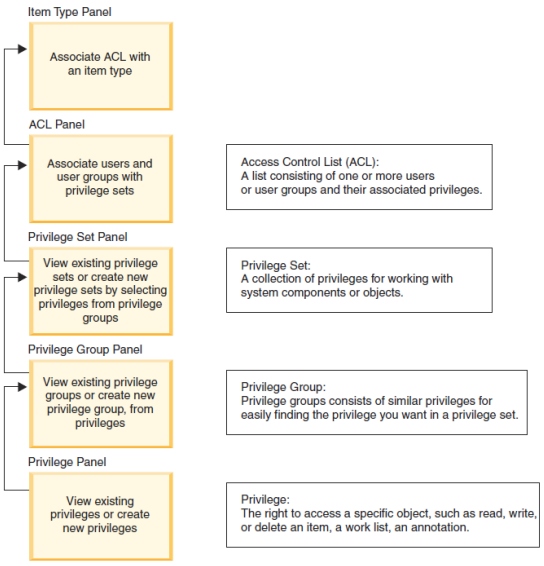
To select the default resource manager, collection, and access control list for the user:

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.

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 object 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.

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.

When you create a user ID, the system automatically assigns it to a predefined user group called **ICMPUBLC**. So, if you want to see all user IDs defined to the system, you can view this user group.



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

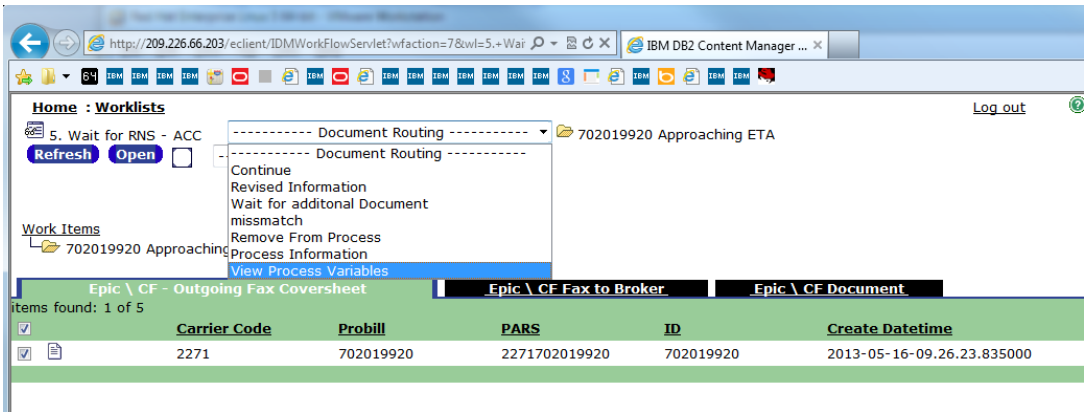
Access control lists: An access control list (ACL) is used as an additional check at run time to determine what create, retrieve, update, and delete operations a user can execute. An ACL is a list consisting of one or more individual user IDs

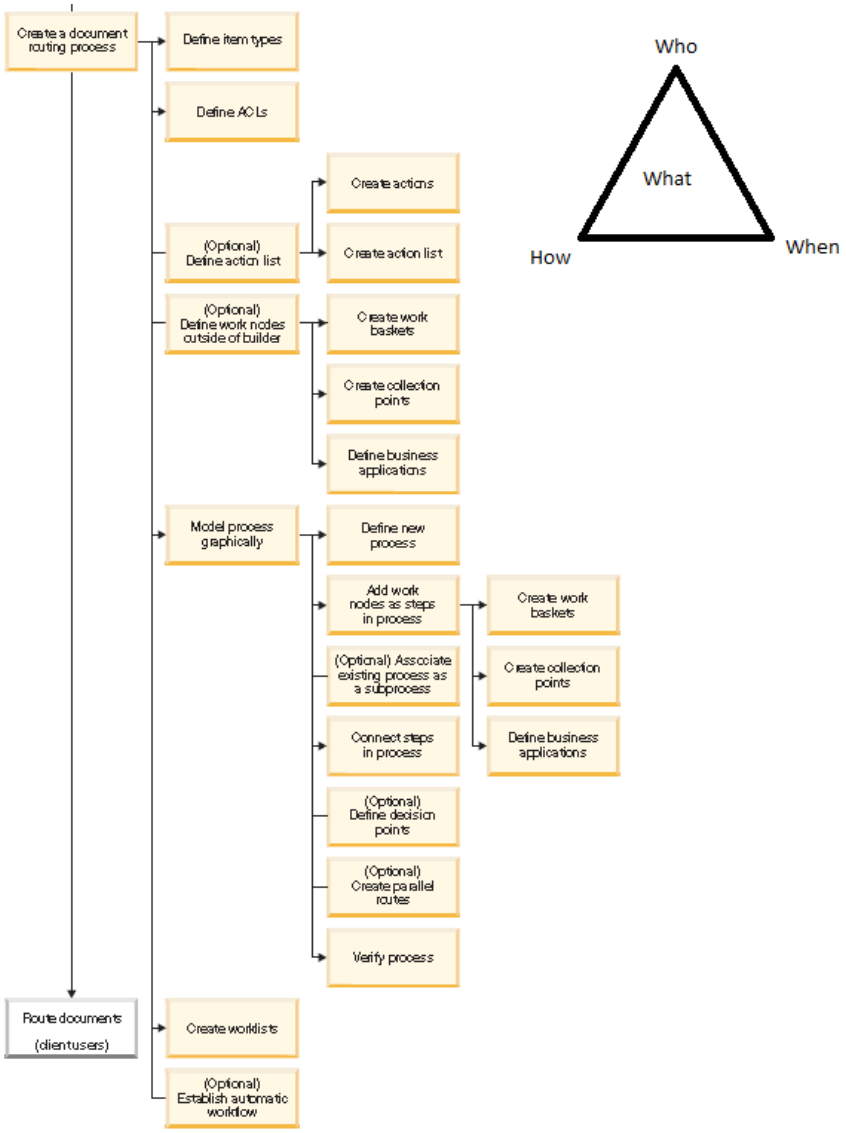
or user groups and their associated privileges. You use ACLs to control user access to objects in the system. The objects that can be associated with access control lists are: the data objects stored by users, item types and item type subsets, worklists, and processes.

Document Routing

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.

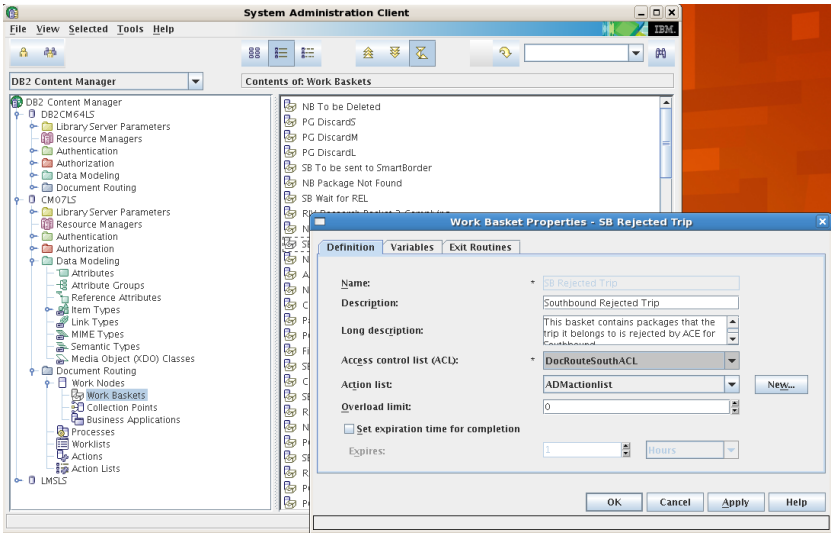
Document routing is a work management tool that you use to direct documents and folders from one user to another during the life cycle of a document.

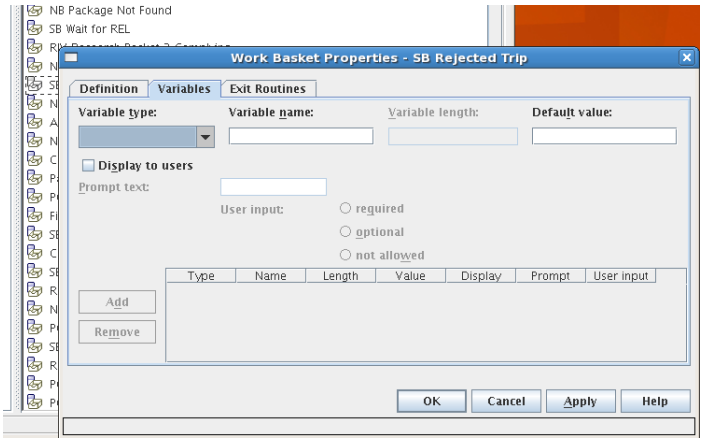


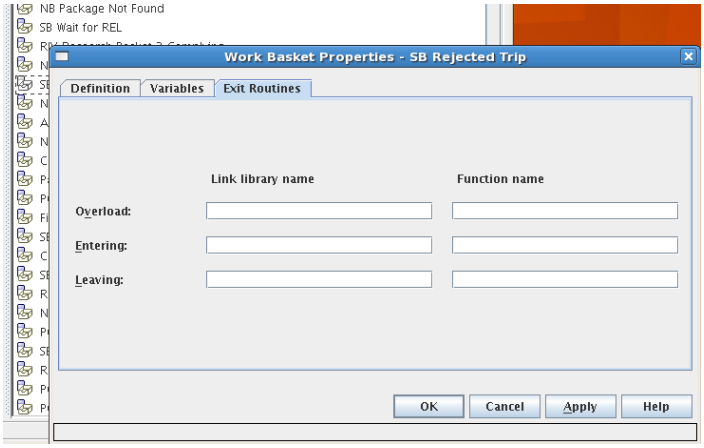


Identify the **work nodes** (work baskets, collection points, and business applications), any decision points, and any subprocesses required for your process. You can also identify points in your process where the process splits into parallel routes and then where it joins back into a single route. You define these document routing elements when you build your process.

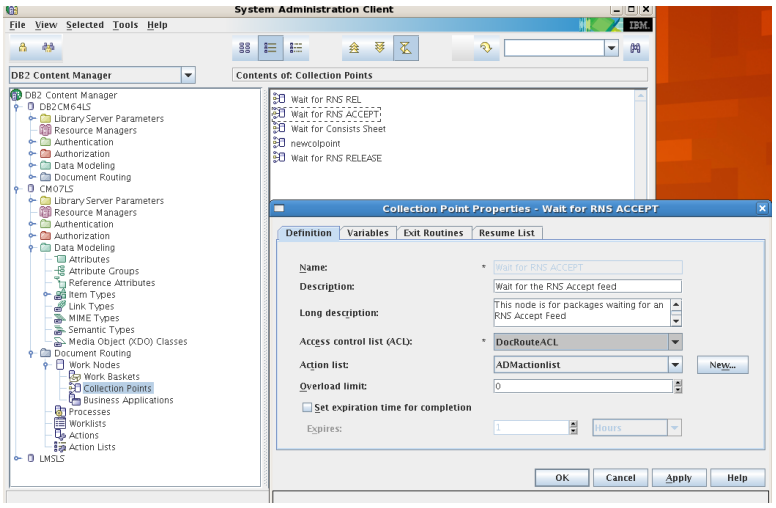
Work baskets (A work basket is a location at which work waits for action by a user or an application. The action can either be taken on the work waiting at the work basket, or the action could be routing the work to another work node)



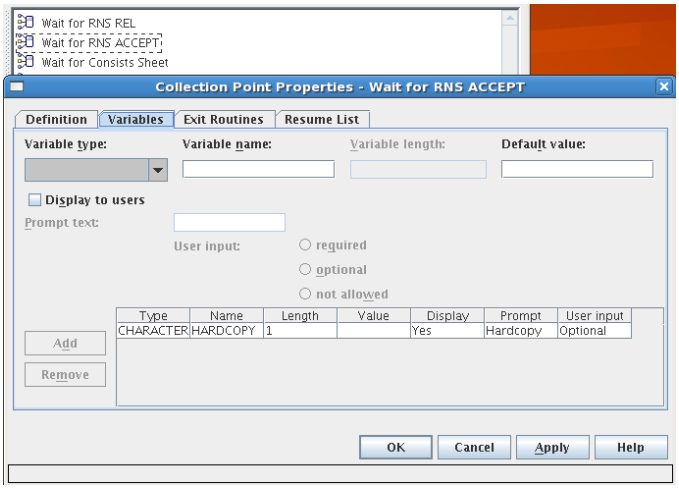




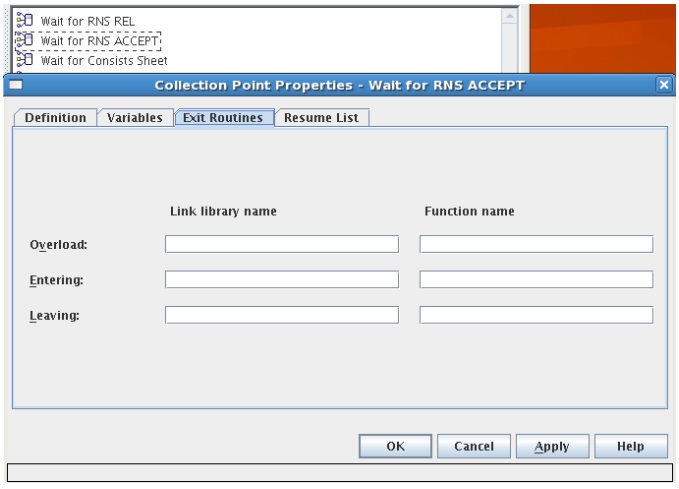
Collection Points (A collection point is a special work node at which a specified folder waits for arrival of other specified documents or folders. Documents or folders flow through the collection point without stopping if either a folder of the specified type is not waiting at the collection point or, if the documents or folders that reach the collection point are not of the specified type to wait for. 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)



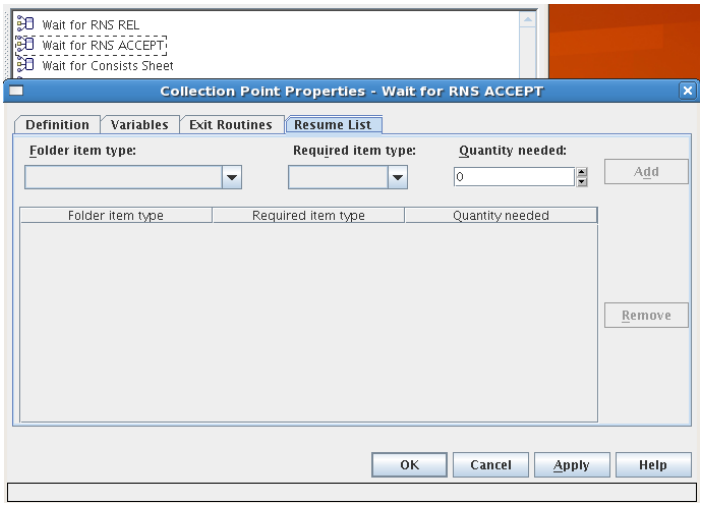
Variables



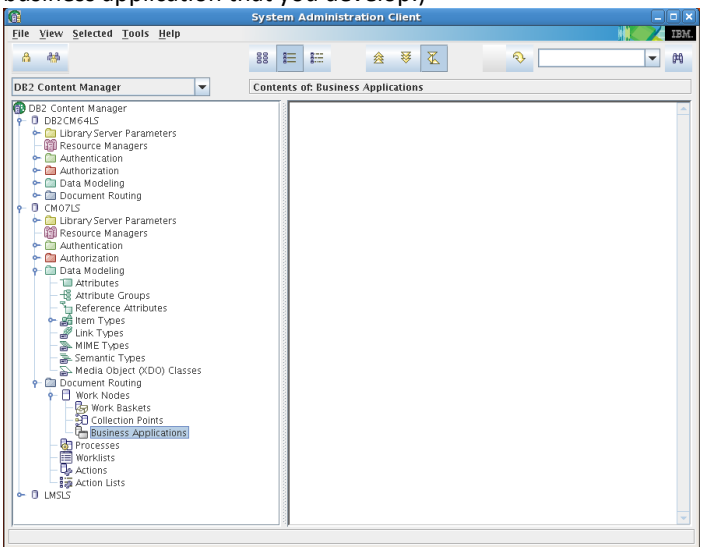
Exit Routines



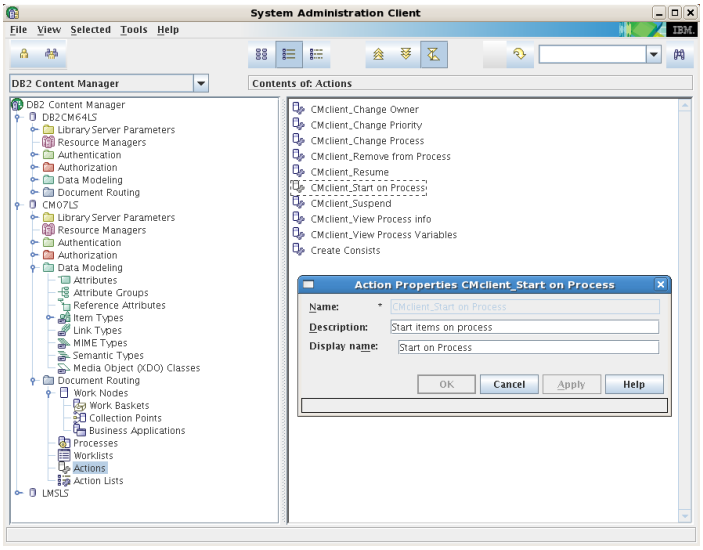
Resume List

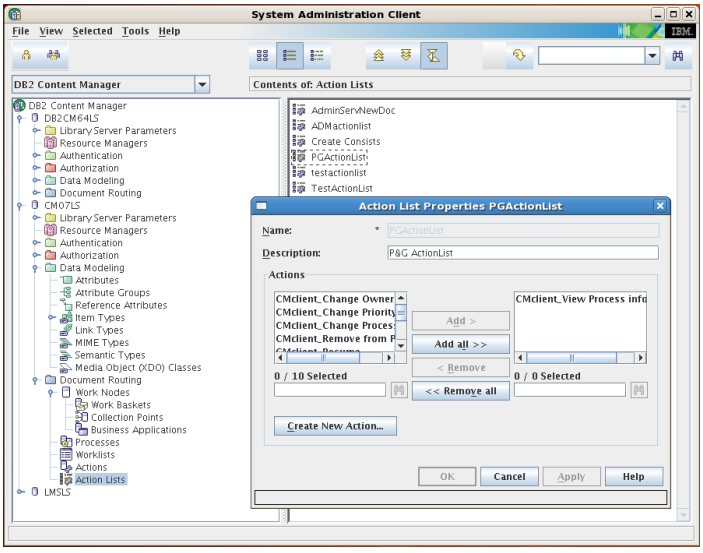


Business Applications (A business application node (LOB node) is a work node that directs work packages to an external business application that you develop.)

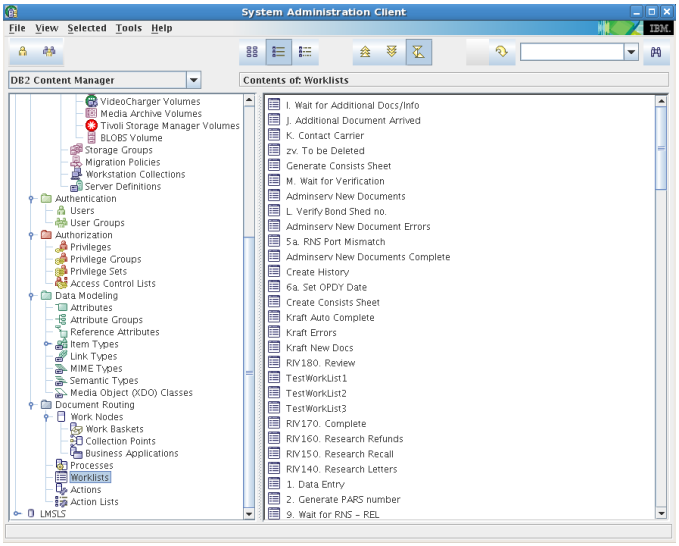


Define an **action list** if you want to identify specific **action**s for client users to perform during the steps in your process. You can select from a set of predefined actions and create your own actions. The actions that you create become menu choices that client users can select while working with your process.

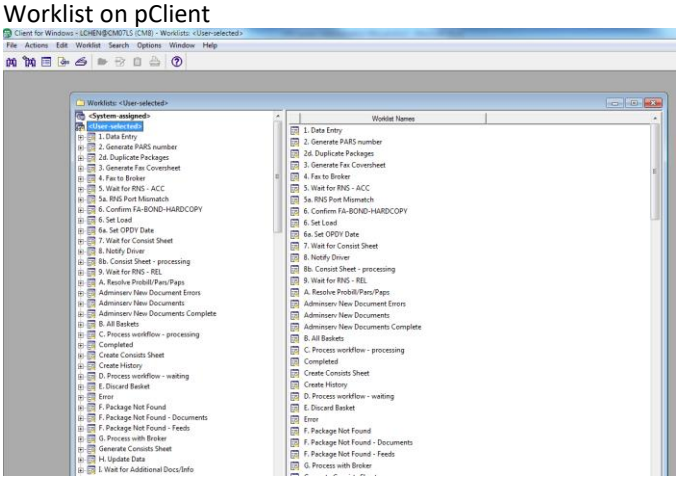




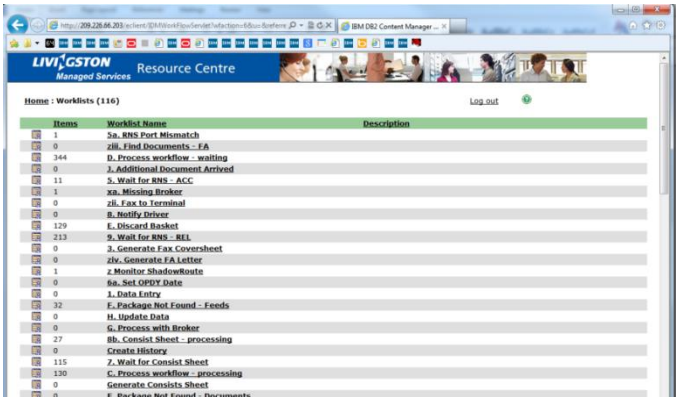
Work lists: You define a worklist to filter **work packages** that are available to your **users**. From the Client for Windows(pClient), eClient, or a custom client, your users access the document routing process from the worklist. Users complete required activities (which you defined with the work 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.



Worklist on pClient



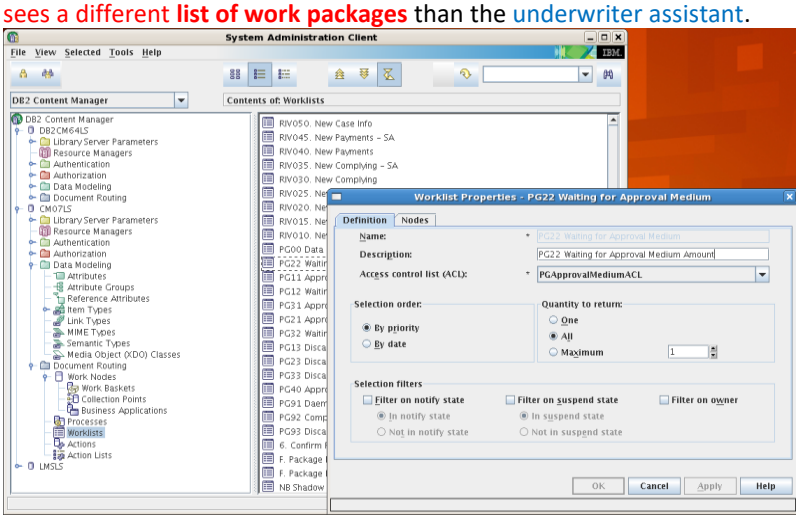
Work Lists on eClient:

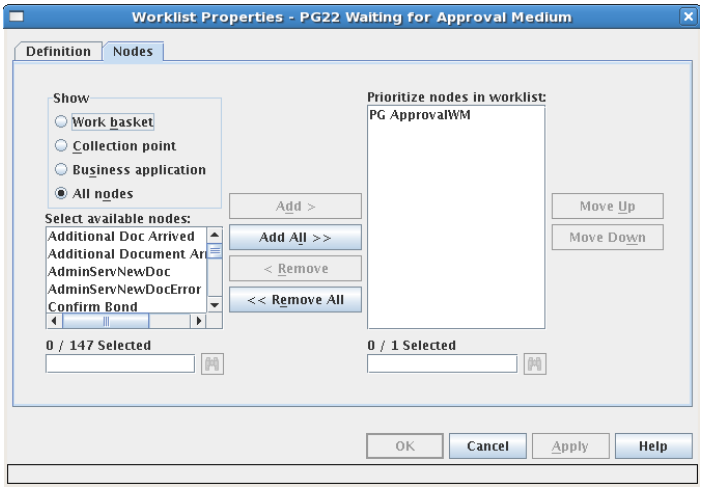


A worklist spans all work nodes, regardless of process. Work packages are prioritized in the worklist based on the priority of the **work nodes** specified in the list and on **other criteria that you select**, such as priority or work package creation date.

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.

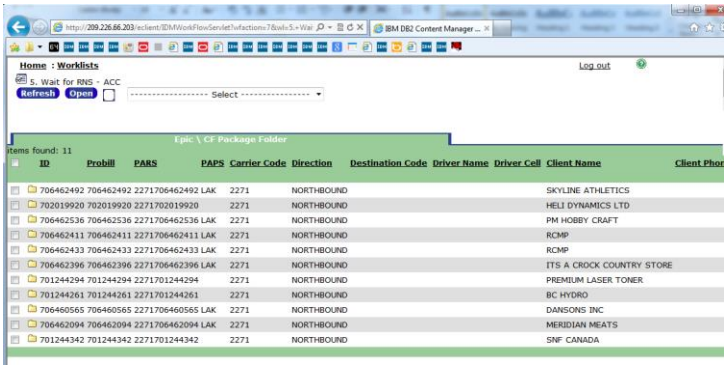




Work package: A work package contains the information that a user needs to complete a task. The user is unaware of a work package because the user works on the item it references, not on the work package itself. Work package properties include a set of information about the item or items being routed 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.

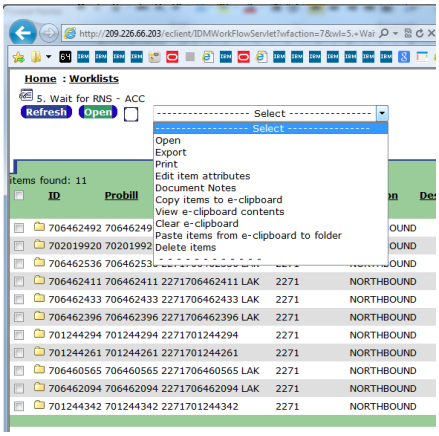
Work packages are created by the system with information from the user who starts a process (**You do not create work packages**).

Check the content(work package) of one example worklist: wait for rns

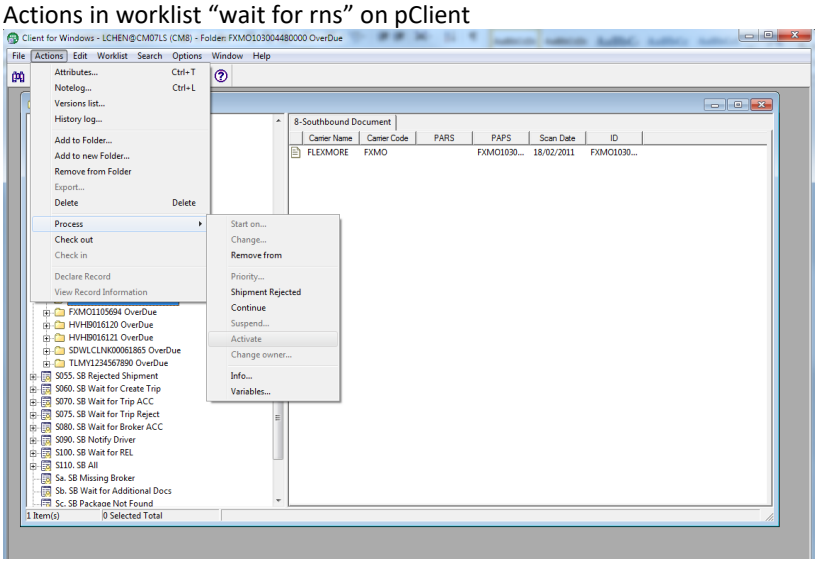


During the process: Although you are not required to define an **action list**, if you do not, your users see only menu choices related to the available routes for the work package; these route names might be cryptic.

Actions in worklist “wait for rns” on eClient



Actions in worklist “wait for rns” on pClient

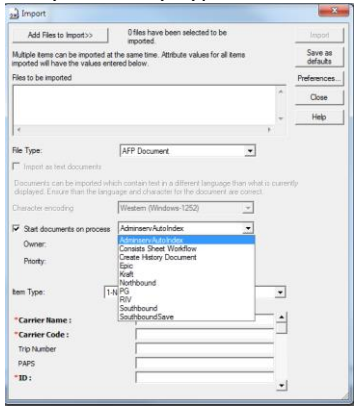


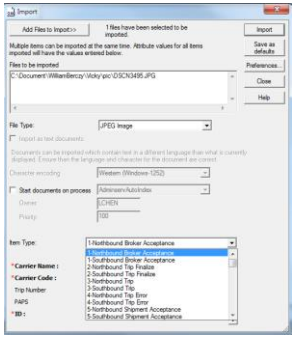
An **access control list** consists of users and user groups and privileges as CRUD (create, retrieve, update, and delete) associated with each. Apply an ACL to any of the following document routing process elements: item types, work nodes, worklists, and the process itself.

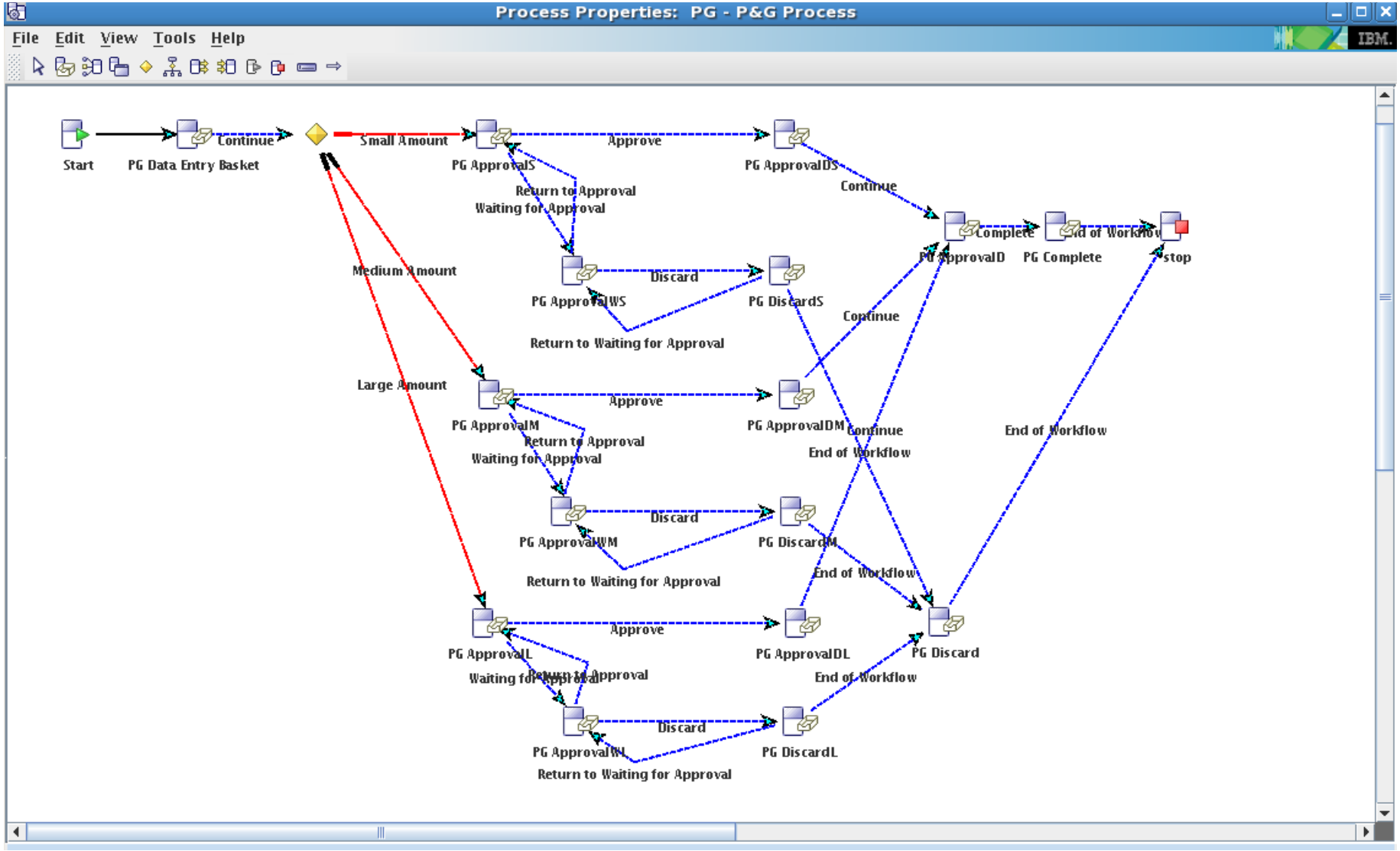
When you associate an access control list with an **element**, only the users on that list can access objects created in the system under this item type. The actions that users can perform on these objects depends on the privileges associated with them in the access control list.

Processes: 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.

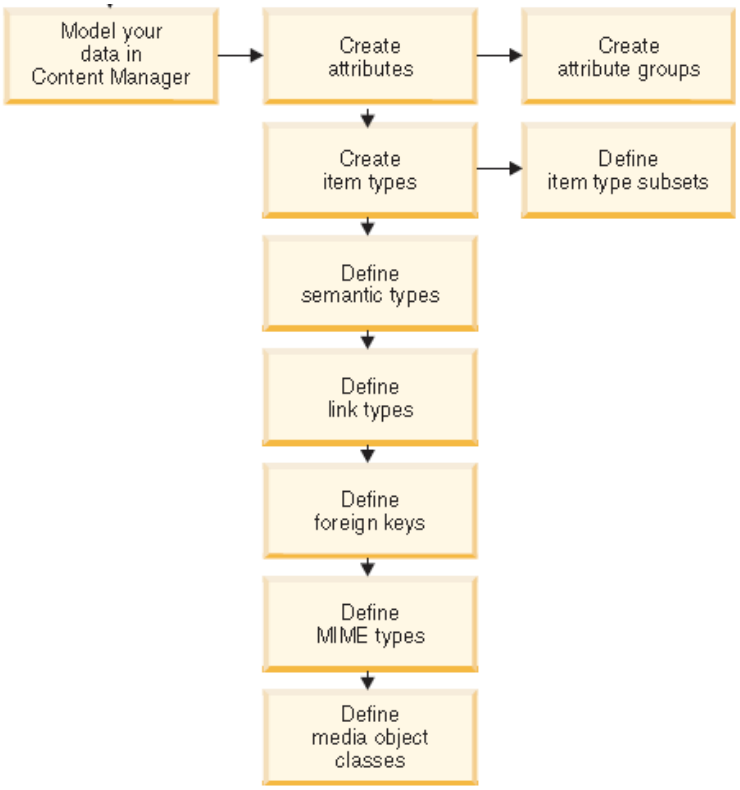
To start a process, pClient/eClient Scan/Import a file, select File Type, Start documents on process, Itme Type, Carrier Name, Carrier Code, Trip Number, PAPS, ID , Entry No, Entry Type, Broker File Nnumber, Broker Accepance DateTime, PARS, Create Datetime:



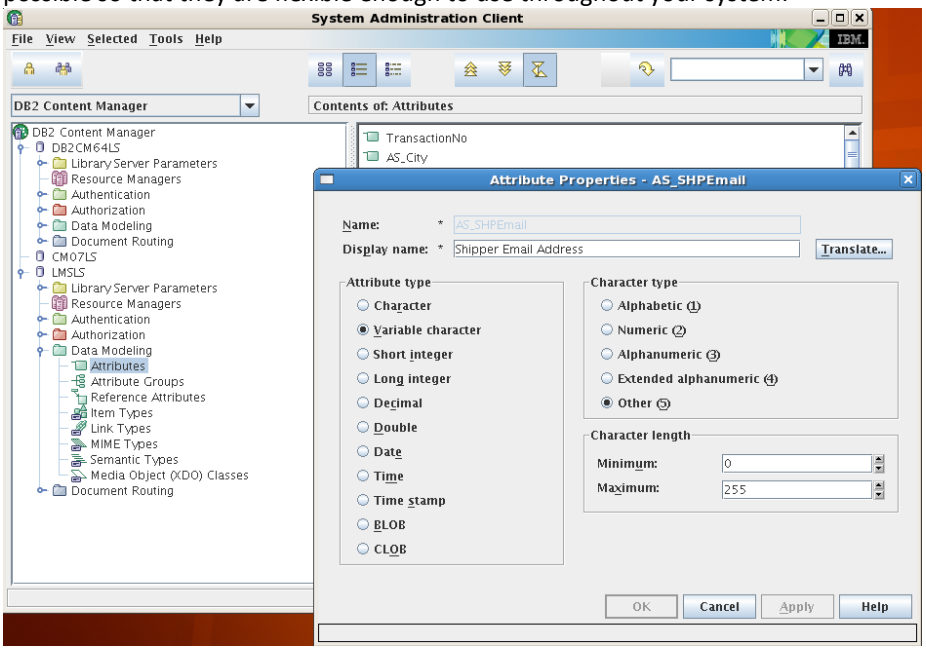



Process Properties: PG - P&G Process
File Edit View Tools Help
IBM
Start
PG Data Entry Basket
Continue
Small Amount
PG ApprovalS
Approve
PG ApprovalDS
Return to Approval
Waiting for Approval
Continue
Complete
PG ApprovalD
PG Complete
stop
Medium Amount
Discard
PG ApprovalWS
PG DiscardS
Return to Waiting for Approval
Continue
Large Amount
PG ApprovalM
Approve
PG ApprovalDM
Return to Approval
Waiting for Approval
Continue
End of Workflow
End of Workflow
Discard
PG ApprovalWM
PG DiscardM
Return to Waiting for Approval
End of Workflow
PG ApprovalL
Approve
PG ApprovalDL
PG Discard
Waiting for Approval
End of Workflow
Discard
PG ApprovalWL
PG DiscardL
Return to Waiting for Approval

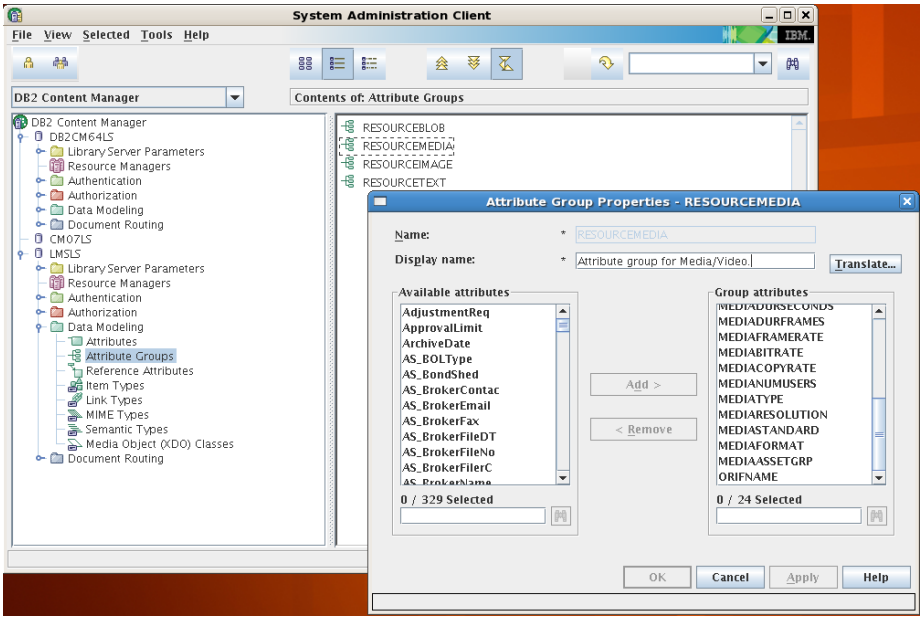
Data Modeling



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.

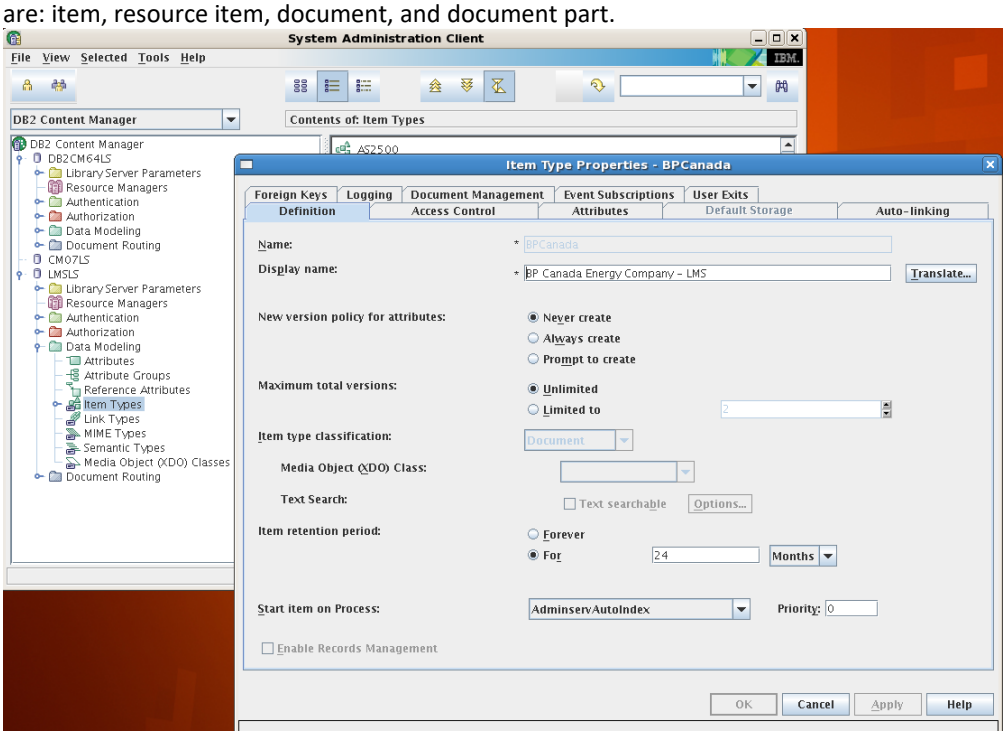


You might find that you often use some of the same attributes together. For these attributes, you can create an attribute group. An attribute group is a set of attributes that are grouped for convenience.



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.

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.



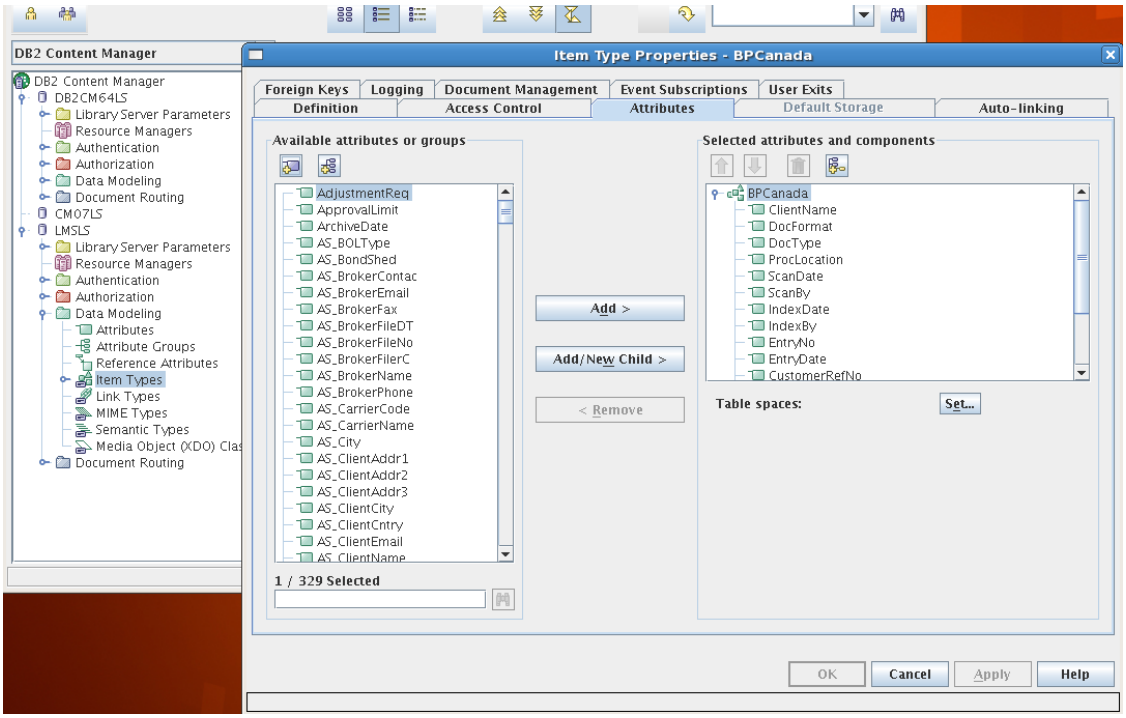
Item type classification, specify the new item type as an item, resource item, document, or document part. By classifying the item type, you make a judgement about the purpose of the items created with this item type.

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.

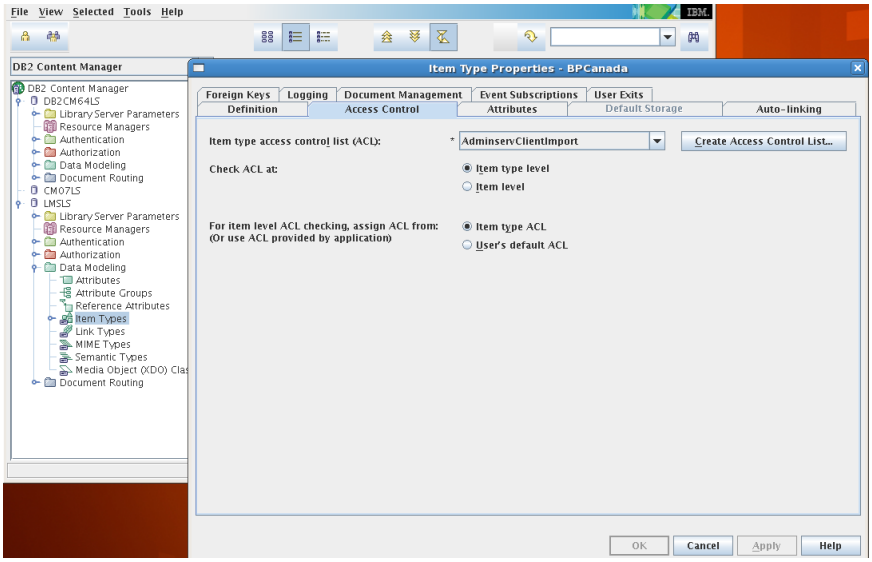
Resource: A resource item describes and provides a connection to content that is stored on the resource manager. For example, resource items might contain pictures. If you select the resource item classification, select a media object class for the item.

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.

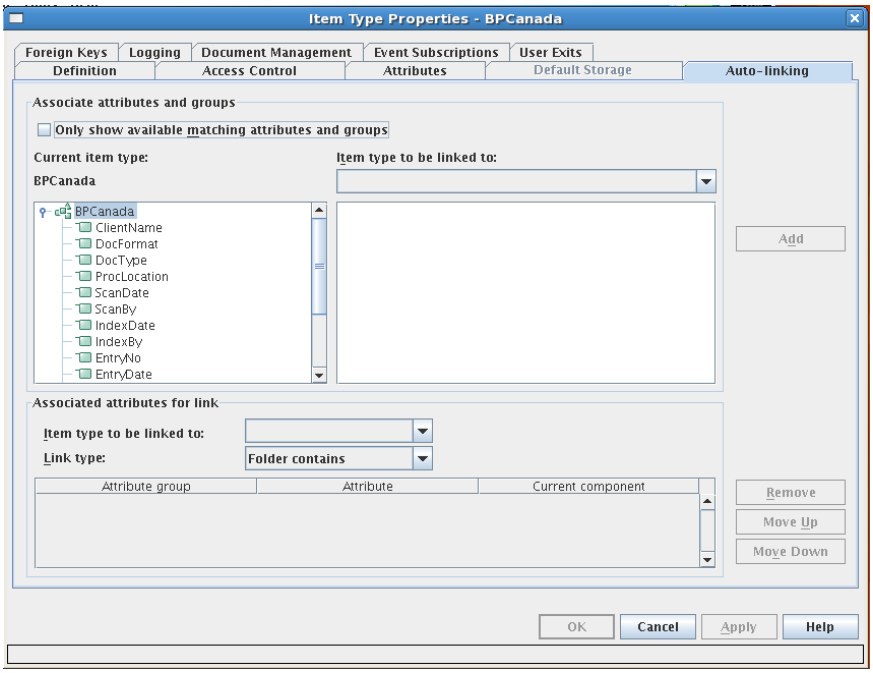
Document part: You associate document parts with a document item type. You can associate any given document part item type with only one document item type. You associate document parts with a document in the Define Document Management Relations window, which you reach by clicking Add on the Document 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.



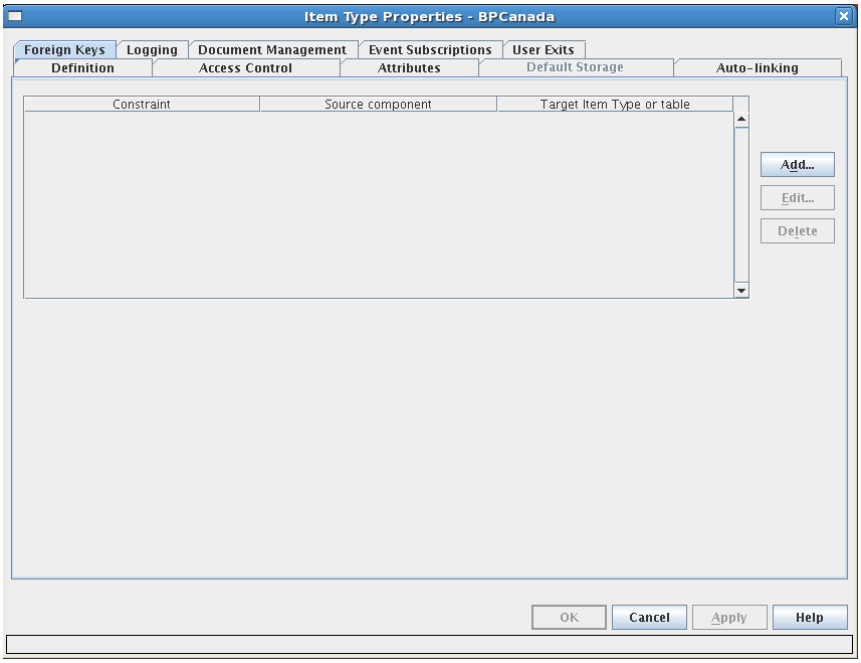
An **access control list** consists of users and user groups and privileges as CRUD (create, retrieve, update, and delete) associated with each. Apply an ACL to any of the following document routing process elements: item types, work nodes, worklists, and the process itself.



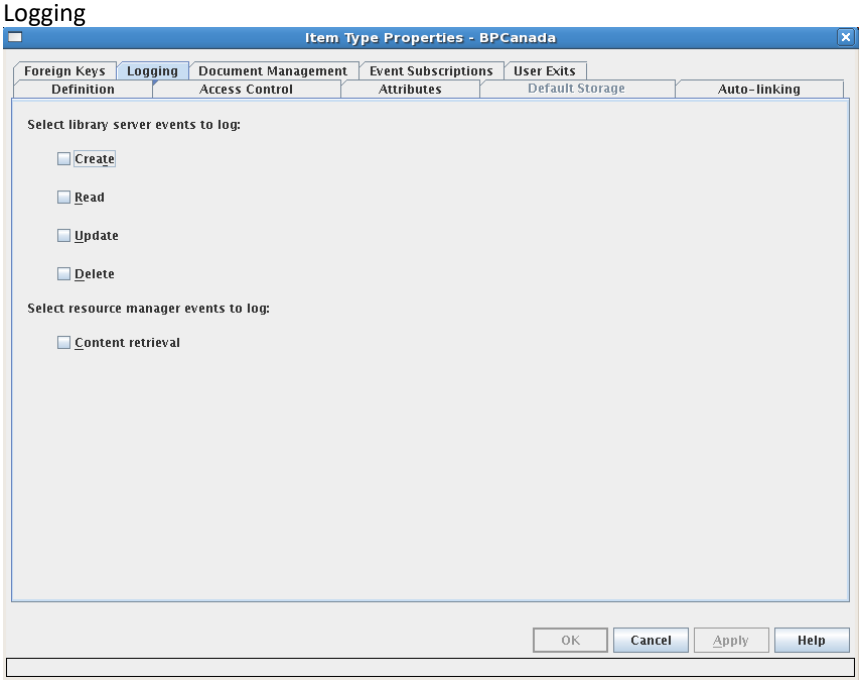
Auto-linking



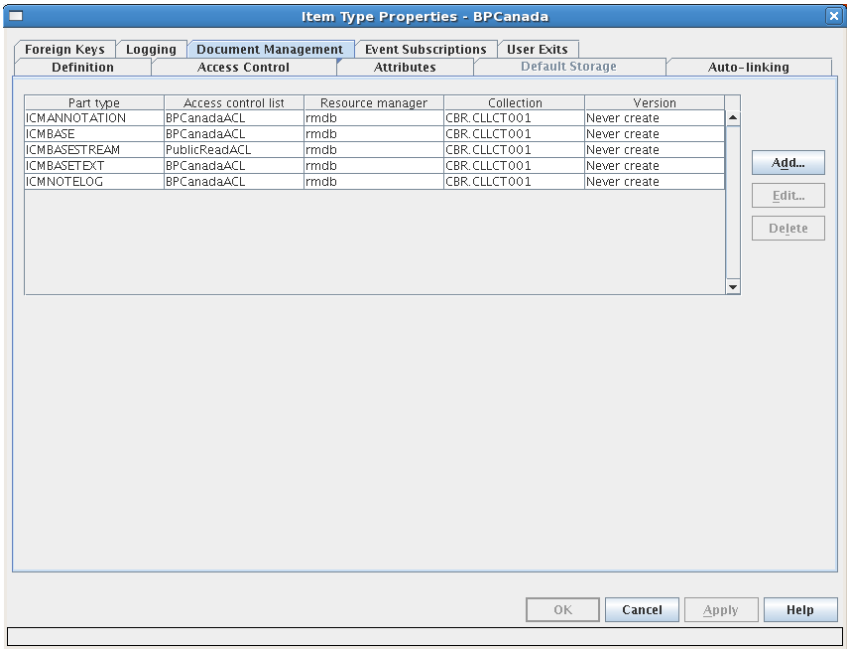
Foreign Keys



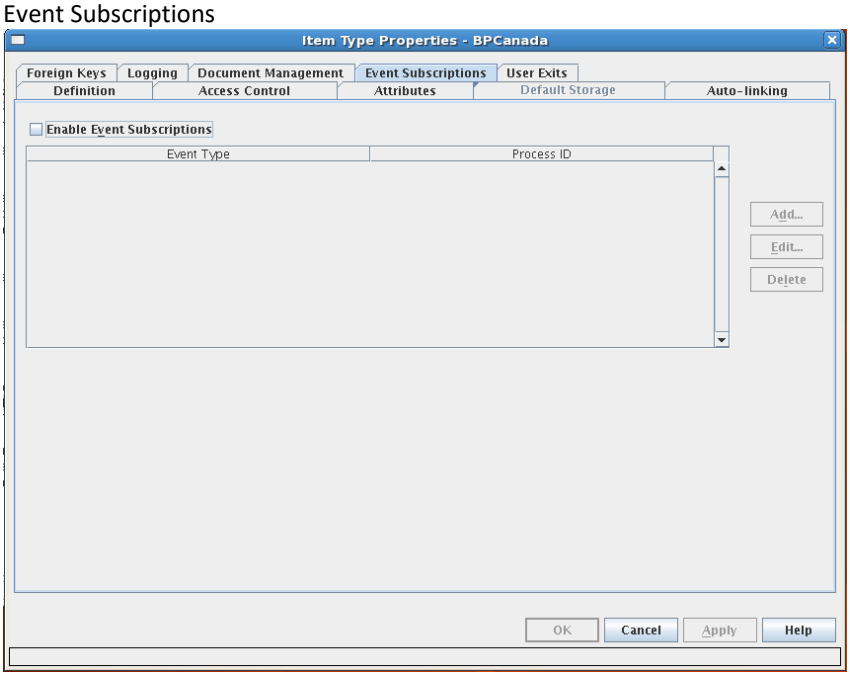
Logging



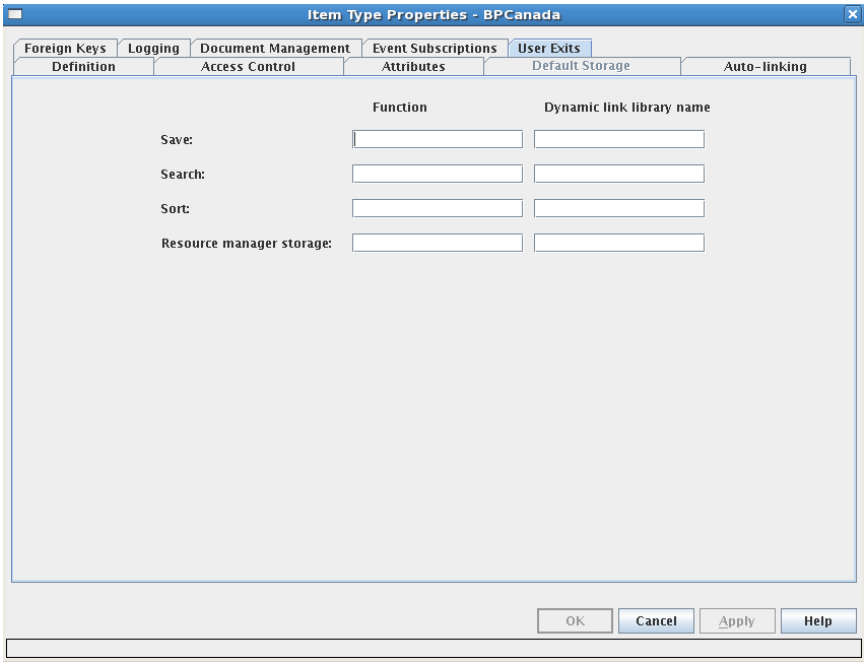
Document Management



Event Subscriptions



User Exits



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.

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.

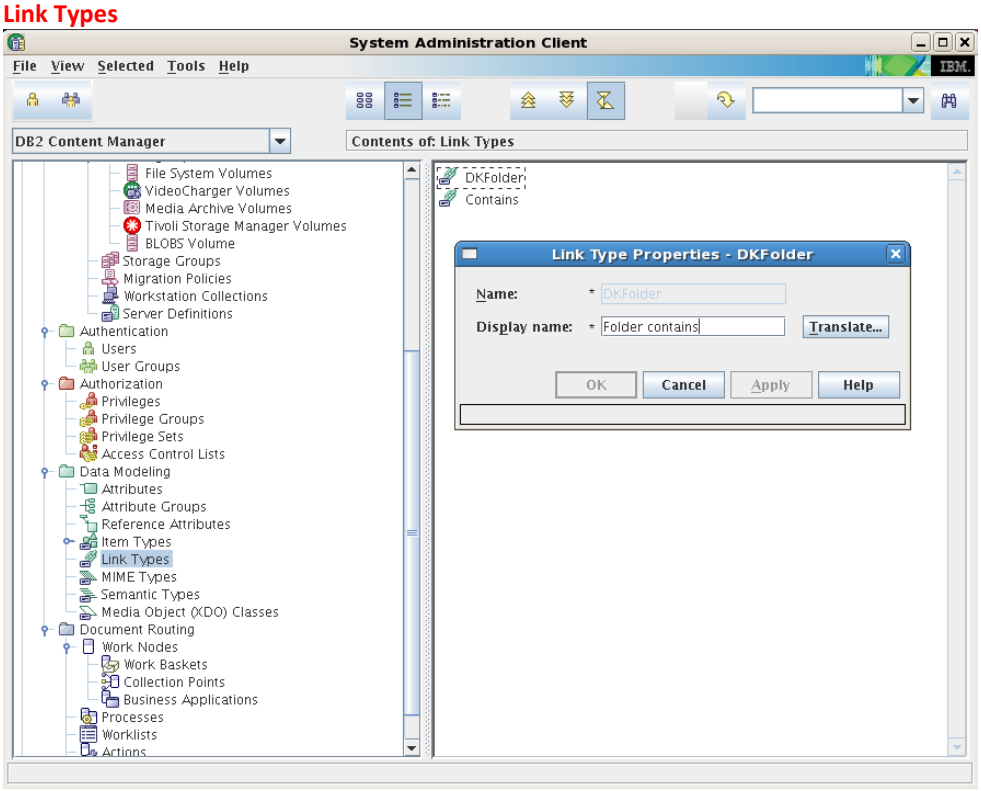
In the Client for Windows, as in earlier versions, the **item type subset is called the item type view or view**. Client for Windows users can see the views that they have access to on the Views page of the Preferences notebook.

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.

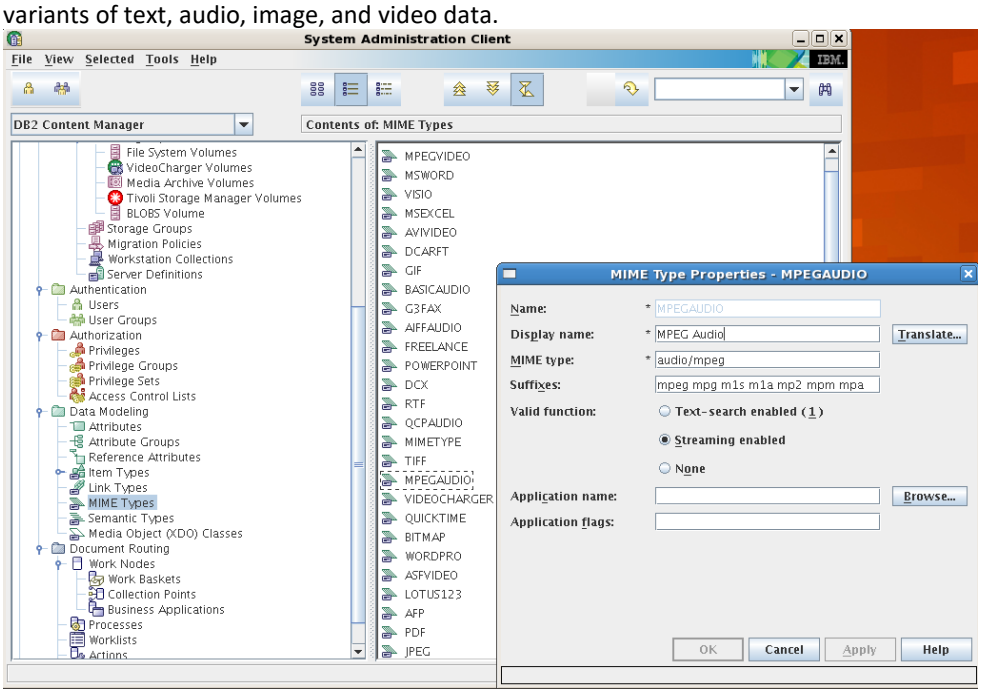
Define **a link type** to provide a custom link relationship that you can use in your custom client applications

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
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

Link Types

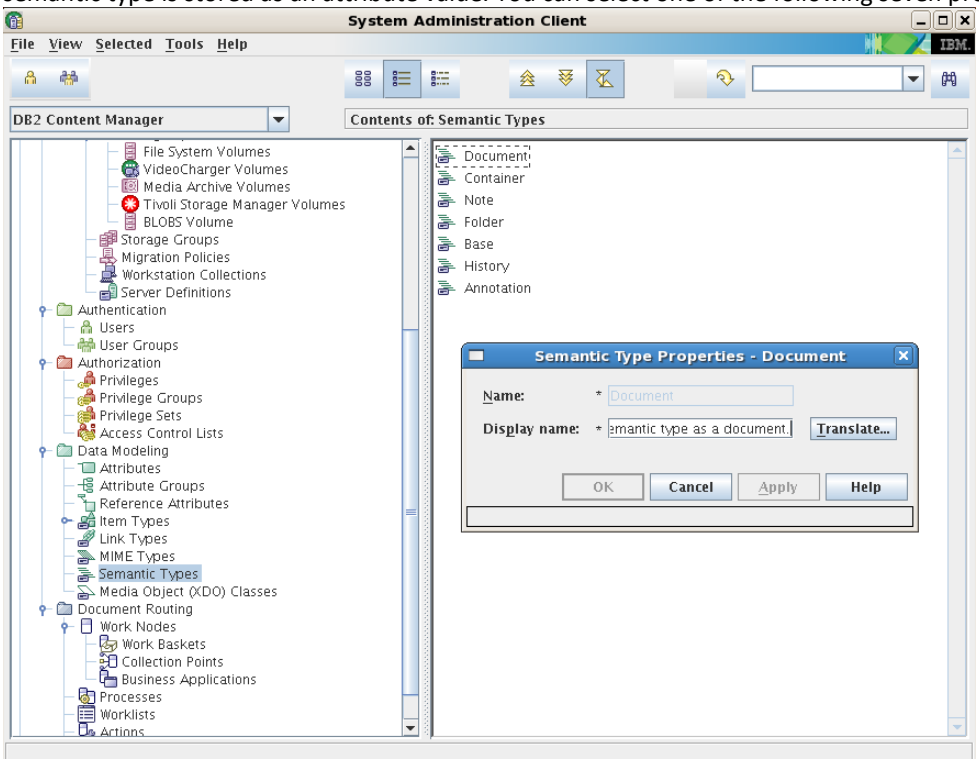


MIME Types: Define the MIME type to tell your application how to handle an object retrieved from the resource manager. when you create an object, you specify its MIME type. When an object of that type is retrieved from the resource manager, your application reads the MIME type and determines how to handle 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.

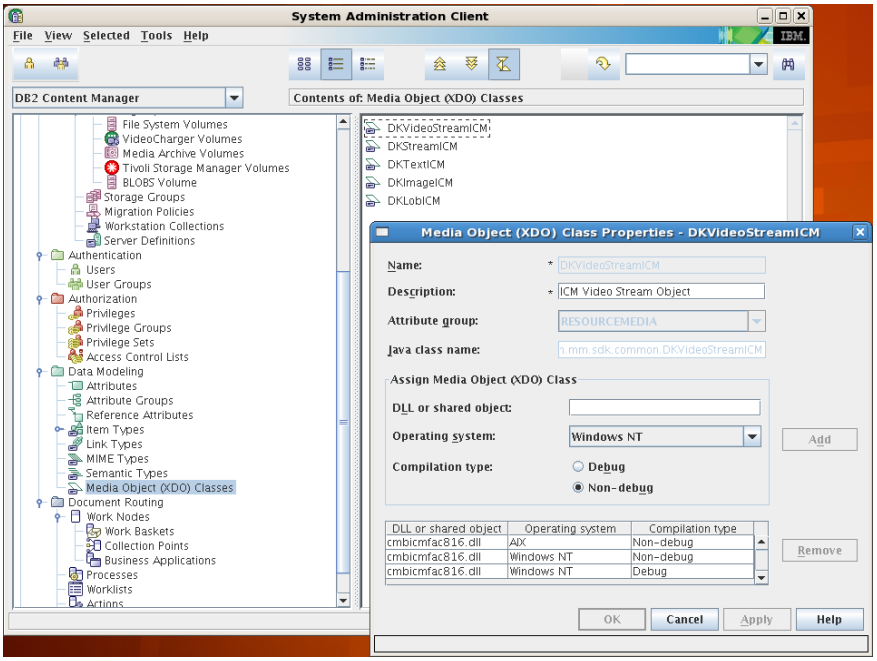


Semantic Types: The semantic type is a descriptive attribute for an item that helps applications to identify the behavior (semantics) for that item. Client applications use the semantic type to distinguish the use and purpose of different items. For example, you might use a document item type to store 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:



Media Object (XDO) Classes: 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



Client for Windows

eClient

LDAP

Java and C++ APIs
HTTP server requests

LMS Maintenance

Once a Content Manager system has been designed, installed, and configured, it is still important to perform maintenance tasks regularly.

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.
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.

By maintaining a Content Manager system properly and in a timely manner, you can get the best possible performance from it over time, and you will potentially avoid problems that can manifest themselves as system endangering situations.

The regular maintenance tasks include the following activities:

- Optimizing server databases: Make sure the Resource Manager and Library Server databases are optimized regularly.
- Monitoring LBOSDATA directory size: This includes local and remote storage devices
- Managing staging directory space
- Removing entries from the events table
- Removing log files: Regularly delete log files that you do not need anymore, to prevent them taking up space unnecessarily. This is particularly important when you enable tracing, as the log files will grow in size extremely quickly
- Managing Resource Manager utilities and services: Make sure the Resource Manager utilities and services that you need in your environment are running and performing their job as expected
- Replacing or repartitioning a hard disk
- Backup: Back up critical components on a regular basis, and test that these backups work on a regular basis by restoring your system to another machine

Optimizing server databases

Database statistics should be updated periodically, daily or weekly depending on the ingest load, on the Library Server and Resource Manager databases in order to maintain good performance. This should also be the first step whenever it appears that there are problems associated with Library Server performance, such as slower logons, searches, or indexing.

RUNSTATS/REBIND database tables

Keeping DB2 statistics up to date on the tables and data helps the optimizer to choose the best execution access plans for SQL statements to maximize performance. We recommend that you run RUNSTATS and REBIND commands on a regular basis as part of regular database maintenance. Recalculating table statistics is critical to improving database performance and should be done *regularly*. If a recalculation of table statistics has not been done recently, then this should be the first step in diagnosing DB2 performance issues.

REORGCHK/REORG database tables

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.

You can synchronize the data in the index with the database tables by running the REORGCHK command in DB2. The REORGCHK command gathers and compares both the index and the table statistics and recommends tables to reorganize.

Jobs	Scripts name	Scheduled by	scheduled running time	logs	Email Distribution
runstats & rebind	/admsrv/db2/icmnlsdb/db2stats/ls_stats.ksh	db2inst1	3:45AM Every Saturday	/admsrv/db2/icmnlsdb/db2stats/ls_stats.out	AIXSupport@livingstonintl.com
	/admsrv/db2/icmnlsdb/db2mgmt/reorgchk/ls_reorgchk.ksh	db2inst1	5:00AM, 1st day Every month	/admsrv/db2/icmnlsdb/db2mgmt/reorgchk/ls_reorgchk.out	AIXSupport@livingstonintl.com

Reorg DB tables	/admsrv/db2/rmdb/db2stats/rm_stats.ksh	db2inst2	3:45AM Every Sunday	/admsrv/db2/rmdb/db2stats/rm_stats.out	AIXSupport@livingstonintl.com
	/admsrv/db2/rmdb/db2mgmt/reorgchk/rm_reorgchk.ksh	db2inst2	5:00AM, 2nd day Every month	/admsrv/db2/rmdb/db2mgmt/reorgchk/rm_reorgchk.out	AIXSupport

Monitoring LBOSDATA directory size

The LBOSDATA directory is an area of local disk that a Resource Manager controls, and is used to store objects.

```
root@admsrv1:/ # df -k
Filesystem    1024-blocks      Free %Used    Iused %Iused Mounted on
/dev/lbosdata01lv  102236160  5196096  95%   740968    39% /lbosdata01
/dev/lbosdata02lv  102236160  5801196  95%   856524    40% /lbosdata02
/dev/lbosdata03lv  102236160  5768980  95%   948215    43% /lbosdata03
/dev/lbosdata04lv  102236160  5268644  95%   774111    40% /lbosdata04
/dev/lbosdata05lv  102236160  5004976  96%   650335    37% /lbosdata05
/dev/lbosdata06lv  102236160  3774552  97%   706285    43% /lbosdata06
/dev/lbosdata07lv  102236160  4643996  96%   697666    40% /lbosdata07
/dev/lbosdata08lv  102236160  3213820  97%   781856    50% /lbosdata08
/dev/lbosdata09lv  102236160  5550720  95%   707064    37% /lbosdata09
/dev/lbosdata10lv  102236160  4252604  96%   571674    38% /lbosdata10
/dev/lbosdata11lv  102236160  5720928  95%   596858    32% /lbosdata11
/dev/lbosdata12lv  102236160  4670260  96%   575057    36% /lbosdata12
/dev/lbosdata13lv  102236160  2157804  98%   474015    50% /lbosdata13
/dev/lbosdata14lv  102236160  4409032  96%   457528    32% /lbosdata14
/dev/lbosdata15lv  102236160  4564016  96%   466530    32% /lbosdata15
/dev/lbosdata16lv  102236160  2775376  98%   436707    42% /lbosdata16
/dev/lbosdata17lv  102236160  3151344  97%   423367    38% /lbosdata17
/dev/lbosdata18lv  102236160  1668932  99%   389857    52% /lbosdata18
/dev/lbosdata19lv  102236160  4174048  96%   406254    31% /lbosdata19
/dev/lbosdata20lv  102236160 21466292  80%   351471     7% /lbosdata20
/dev/lbosdata21lv  102236160 37450108  64%   295421     4% /lbosdata21
/dev/lbosdata22lv  102236160 37123836  64%   294495     4% /lbosdata22
/dev/lbosdata23lv  102236160 37281528  64%   294941     4% /lbosdata23
/dev/lbosdata24lv  102236160 37849800  63%   295046     4% /lbosdata24
```

When using fixed disk attached to the Resource Managers for object storage, it is very important to make sure that there is enough free space remaining for Content Manager to write objects to. If Content Manager runs out of space to write objects to, any new requests to store objects will fail.

Even when Tivoli Storage Manager (TSM) is used for the long term storage of objects (NOT implemented in current LMS environment), Content Manager may be configured to keep objects locally, and only migrate to TSM after a period of time (for example, 30 days). The migration of objects to TSM is triggered by the length of time the objects have resided in the first storage class, assuming there are only two storage classes and TSM is the second one.

It is possible that the local fixed volume that the LBOSDATA directory resides on, may become completely full if new objects are being added to it faster than they are being migrated to TSM by the Content Manager Migrator process. This may occur during peak periods of object loading into Content Manager, such as around the end of a financial year for an accounting company that scans documents into Content Manager for reference purposes. In worst case scenario, the process of migrating from LBOSDATA directory to TSM may not even be running.

During peak activity times, it is even more important to monitor the amount of free space remaining within the local fixed disk that the LBOSDATA directory resides on. Of course, these peak periods of activity should have been taken into account when designing and sizing the system; nevertheless, monitoring the directories is good practice. Operating system tools should be used to monitor the current space occupied by the local objects, and the amount of space remaining on a physical or logical volume.

It is possible to see how many MBs of storage remain on a particular file system volume through the Content Manager System Administration Client; however, this value does not get updated dynamically. If space is being used on a file system volume while you are logged onto the System Administration Client, the number of MBs free on the file system volume will not change. To see the change in volume free space, you need to log off and log back onto the System Administration Client. Note that this is not an entirely accurate way to monitor free space.

[Important]: *It is important to remember to have the Content Manager Migrator process running at all times, even if you do not migrate objects between storage classes. That is because it is used to physically delete objects from where the Resource Manager has stored them. When an end user deletes an object from the standard client, only the row from the Library Server database is deleted immediately (for performance reasons), the entry in the Resource Manager database and the object itself remain. The migrator must be run to reclaim the physical storage space.*

In the same way, Content Manager does not reserve space for its objects on a file system volume. It is very important to make sure that no other applications use the same volume to store dynamic data. If this occurs, the amount of free space available to Content Manager to write objects can unexpectedly be changed.

Should a file system volume become full, it is possible to define a new volume, assuming you have the physical space available, and then add this new volume to the existing storage group, in order to provide further space for Content Manager to store objects to.

When you define a file system volume, a threshold percentage can be entered. This value is used as a limit at which point Content Manager will attempt to migrate objects to the next storage class, if one exists, and if the migrator process is running. The default value for the threshold is 95%. This threshold limit should never be reached in the normal course of events, and the threshold limit mechanism should not be relied upon as the default way of monitoring and dealing with overly full volumes. In most circumstances, the default value of 95% will be fine to use in a production system.

A more effective way to prevent Content Manager running out of space is to create overflow volumes which are volumes that can be used by any storage groups, when all other storage systems, such as a file system volume, within a storage group are full. To create an overflow volume, select Overflow under the

Managing staging directory space

The staging area is used as a temporary storage area for objects retrieved from TSM storage **(LMS does NOT use TSM as ITEMS storage volumes, nor use LAN Cache Enabled)** as the location to store objects when the LAN cache is enabled for a Resource Manager.

Using the staging area enables faster response time for subsequent retrievals of the same objects.

The System Administration Client allows users to manage the staging directory to get the most benefits from LAN caching and also from TSM object retrieval caching. Staging directory management tasks include:

Setting automatic cache purge specifications: A purge removes the oldest, least frequently used objects from the staging directory.

Purger process example

The purger process is used to maintain the size of the staging area. When the staging area size reaches a preset upper limit, the purger will begin to remove files until it reaches a preset lower limit. For example, our staging area is 199 MB in size and purging will commence when this 199 MB area is 80% (159.2MB) full, providing the purger process is started.
Once the staging area reaches 159.2 MB full in size, the purger will start randomly deleting files until the staging area reaches 60% of 199 MB (119.4MB).
All of the staging area values are configurable. For example, if you want to completely clear the staging area, you can set the start purge size to 1% of the maximum staging area, and the stop purge size to 0% of the maximum staging area size.
With the configuration set, you should be able to clear the entire staging area assuming that the staging area is at least 1% of 199 MB full at the time. If the staging area is below 1% full at the time, you need to reduce the size of the staging area down from 199 MB to a size where 1% of the staging area maximum size was smaller than the currently occupied space within the staging area.
The staging area maximum size and purge rates are monitored periodically, not constantly. For this reason, you may need to wait up to five minutes, the default setting, before changes you have made to the staging area come into effect. The cycle time for this checking is configured via the Resource Manager Configuration window. To open this window, go to the Content Manager System Administration Client, open a Resource Manager and select Configurations. Then select the Resource Manager Configuration that you are currently using, the default is IBMCONFIG, and select the tab labelled Cycles.
The threshold cycle sets the amount of time that elapses before the staging area size is updated. The other cycles refer to amount of time that elapses before the various Resource Manager Utilities check to see if they have any work to do.
The settings for the staging area and cycle times that are best suited to your environment may differ from the default settings. For example, if your system produces instances when the staging area is heavily used, you may need to adjust the cycle time so that the purger checks the staging area more regularly to see if it has any work to do.
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 may need to modify the original parameters defined for the staging directory.

Removing entries from the events table (Schedule it according to your business requirement)

DB2® Content Manager can log system administration and item events for audit purposes. Logging is optional.

From: Sinopoli, Josephine
To: Stanciu, Claudio
Cc: Kim, Richard
Sent: Fri Aug 16 16:55:09 2013

Subject: RE: Regarding Event Table
Hi Claudio,
I spoke to Tracy about this issue and she's ok with purging the History Table data every 2 years. Do you think the command you created below will allow us to keep the data for that time period?
Thanks
Josie

From: Stanciu, Claudio
Sent: Thursday, August 08, 2013 3:32 PM
To: Guo, Denny; Kim, Richard; Sinopoli, Josephine; Farma, Jashan
Cc: Liu, Tony
Subject: RE: Regarding Event Table

The purge command should look like this :

DELETE FROM ICMADMIN."ICMSTITEMEVENTS" where (userid = 'LMSD' or userid = 'ICMADMIN') and eventdata1 = '1' and eventdata2 = '1';

Thanks
Claudio

System administration events include actions performed by an administrator, either within the System Administration client, or in a custom application. These events include defining users, assigning privileges, assigning access control lists to an object, and so forth, 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. To enable or disable logging of system administration events, update the library server configuration.

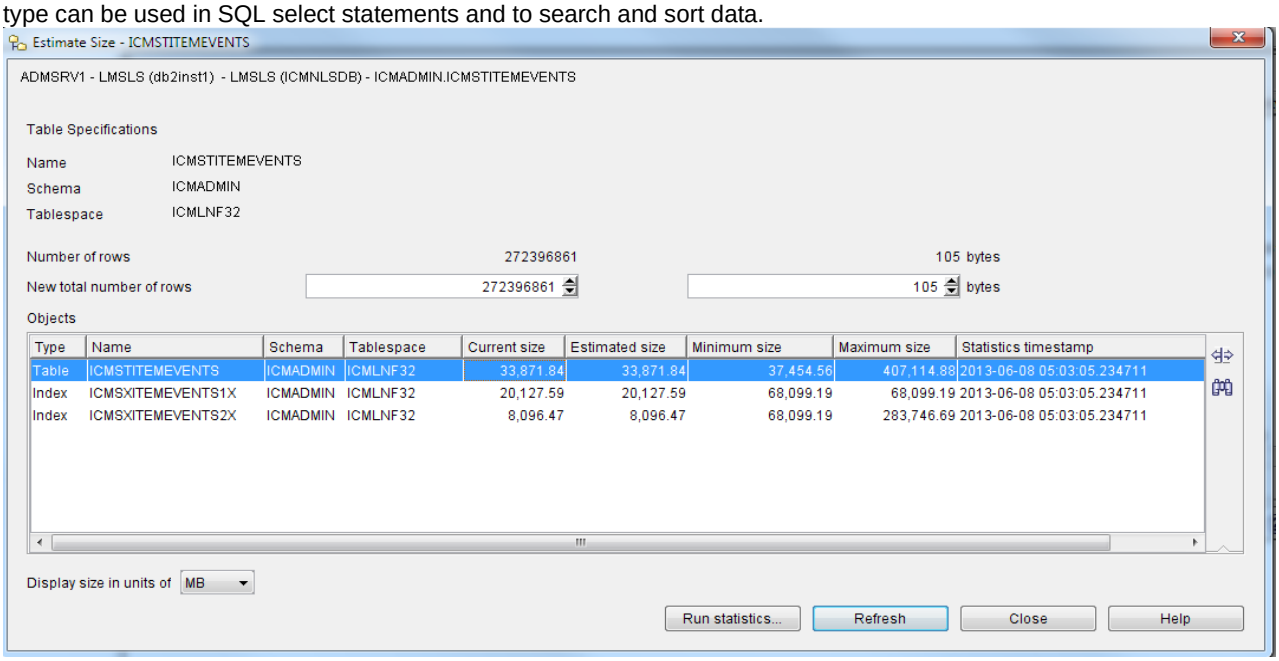
Item events are actions performed against specific objects within the resource manager, or the objects indexing information within the library server. These events are stored in the **ICMSTITEMEVENTS** table. To enable or disable logging of item events, modify the item types you want to log. For each 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).
- The user ID of the user who performed the action.
- 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.

Because the data is stored in DB2 tables, you can issue a variety of 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.



Total size: 62095.9 MB

```
root@admsrv1:/home/db2inst1 > db2 "select count(*) from icmadmin.icmstitemevents where eventcode<=600 and
created < '2000-01-02 00:00:00.000000'"
1
-----------
          0

  1 record(s) selected.

root@admsrv1:/home/db2inst1 > db2 "select count(*) from icmadmin.icmstitemevents where eventcode<=600 and
created < '2010-01-01 00:00:00.000000'”
1
-----------
    1805605

  1 record(s) selected.

root@admsrv1:/home/db2inst1 > db2 "select count(*) from icmadmin.icmstitemevents where eventcode<=600 and
created < '2011-01-02 00:00:00.000000'”
1
-----------
    3636452

  1 record(s) selected.

root@admsrv1:/home/db2inst1 > db2 "select count(*) from icmadmin.icmstitemevents where eventcode<=600 and
created < '2011-01-01 00:00:00.000000'"
1
-----------
    3636164

  1 record(s) selected.

root@admsrv1:/home/db2inst1 > db2 "select count(*) from icmadmin.icmstitemevents where eventcode<=600 and
created < '2013-01-01 00:00:00.000000'"
1
-----------
   82104357

  1 record(s) selected.

//root@admsrv1:/home/db2inst1 > db2 "select count(*) from icmadmin.icmstitemevents where eventcode<=600 and
created < '2013-01-02 00:00:000000’”
1
-----------
   82898771
```

```
  1 record(s) selected.

root@admsrv1:/home/db2inst1 > db2 "select count(*) from icmadmin.icmstitemevents where eventcode<=600 and
created < '2013-01-07 00:00:00.000000’”
1
-----------
   86250070

  1 record(s) selected.

root@admsrv1:/home/db2inst1 > db2 "select count(*) from icmadmin.icmstitemevents where eventcode>=600 "
1
-----------
    4750591

  1 record(s) selected.

root@admsrv1:/home/db2inst1 > db2 "select count(*) from icmadmin.icmstitemevents where eventcode>=900 "
1
-----------
          0

  1 record(s) selected.
```

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

The list of events are as follows:

```
ICM_EVENT_CREATE_ITEM               301
ICM_EVENT_UPDATE_ITEM               302
ICM_EVENT_DELETE_ITEM               303
ICM_EVENT_UPDATE_OBJDATA            305
ICM_EVENT_REINDEX_ITEM              306

ICM_EVENT_GET_ITEM                  401

ICM_EVENT_RETRIEVE_OBJECT           531
ICM_EVENT_REPLACE_OBJECT            532
ICM_EVENT_CHG_SMS_INFO              533
ICM_EVENT_STORE_OBJECT              534
ICM_EVENT_PREFETCH_OBJECT           535
ICM_EVENT_MOVE_OBJECT               536
ICM_EVENT_REPLICATE_OBJECT          537
ICM_EVENT_QRY_SMS_INFO              538
```

1000+
Application event codes

You can delete events from the events table by performing either of these following tasks:
Log in to the server where the database exists.
Open a DB2 command prompt and connect to the library server database.
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 `2010-01-01 12:00:00.000000`. For example:

```
delete from ICMSTSYSADMEVENTS where eventcode <=200 and Created < ‘2011-06-08 05:00:00.000000’
```

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 2010-01-01 12:00:00.000000. For example:

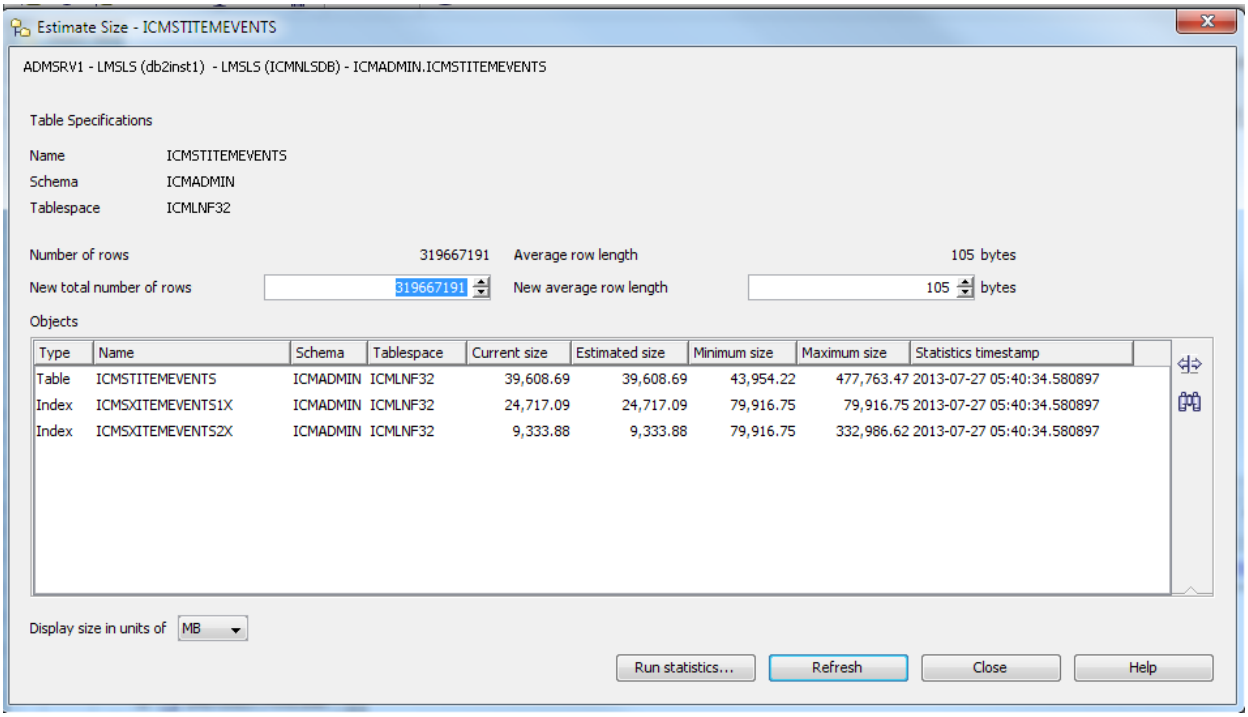
```
delete from ICMSTSYSADMEVENTS where eventcode <=200 and Created < '2005-01-01 12:00:00.000000'
```

Optional: To reclaim the file system space after you delete events, run the database reorganization utility on the library server database and then stop/start the database instance.

Example:

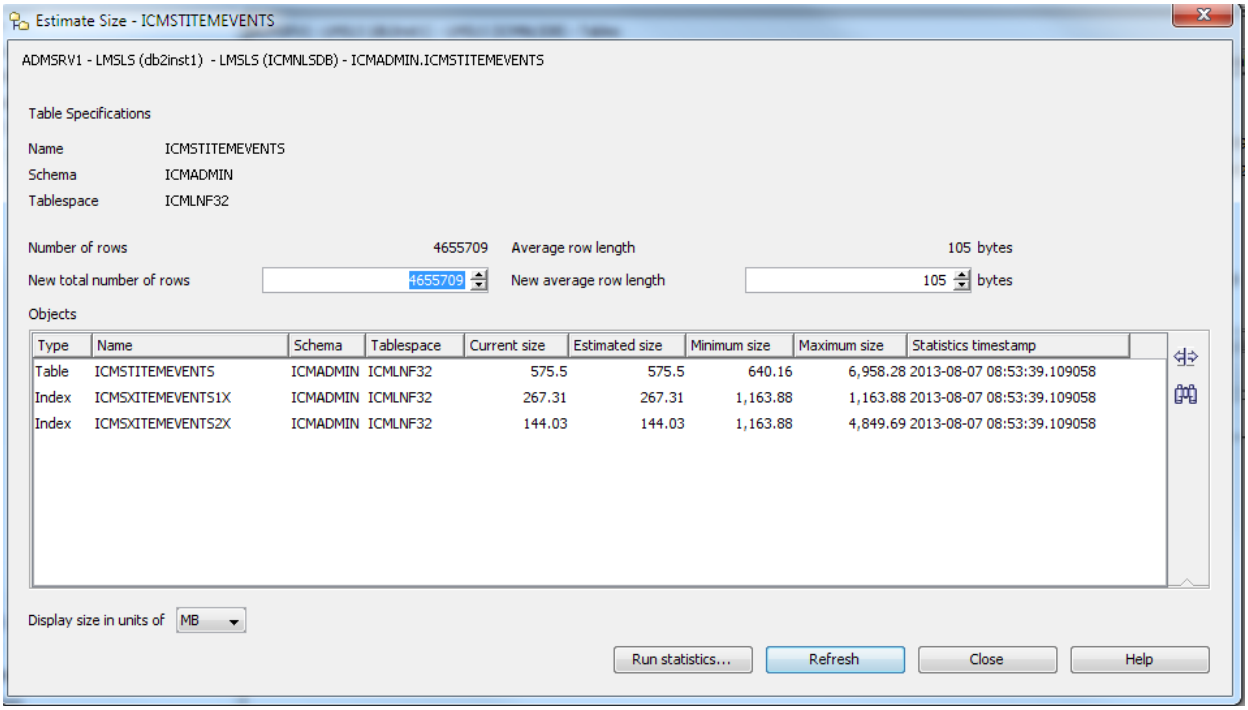
```
db2 export to ICMSTITEMEVENTS.ifx of ixf "select * from from icmadmin.icmstitemevents where
created < '2009-04-01 00:00:00.000000'"

//root@admsrv1:/home/db2inst1 > db2 "delete from icmadmin.icmstitemevents where created <
'2009-04-01 00:00:00.000000'"
DB21034E  The command was processed as an SQL statement because it was not a
valid Command Line Processor command.  During SQL processing it returned:
SQL1024N  A database connection does not exist.  SQLSTATE=08003

//root@admsrv1:/home/db2inst1 > db2 connect to icmnlsdb

   Database Connection Information

 Database server        = DB2/AIX64 9.5.5
 SQL authorization ID   = DB2INST1
 Local database alias   = ICMNLSDB

db2 "delete from icmadmin.icmstitemevents where created < '2009-04-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.
db2 "delete from icmadmin.icmstitemevents where created < '2009-05-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.
db2 "delete from icmadmin.icmstitemevents where created < '2009-06-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.
"delete from icmadmin.icmstitemevents where created < '2009-07-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.
db2 "delete from icmadmin.icmstitemevents where created < '2009-08-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.
db2 "delete from icmadmin.icmstitemevents where created < '2009-09-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.
db2 "delete from icmadmin.icmstitemevents where created < '2009-10-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.
db2 "delete from icmadmin.icmstitemevents where created < '2009-11-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.
db2 "delete from icmadmin.icmstitemevents where created < '2009-12-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.
db2 "delete from icmadmin.icmstitemevents where created < '2010-01-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.

Last SQL:
db2 "delete from icmadmin.icmstitemevents where created < '2011-00-01 00:00:00.000000'"
DB20000I  The SQL command completed successfully.

df -k show 85% usage of /home/db2inst1, no space usage change after the table clean
```

Reorganizing tables online



Reorganizing tables offline is the fastest way to defragment your tables. Reorganization reduces the amount of space that is required for a table and improves data access and query performance.

```
CONNECT TO ICMNLSDB;
REORG TABLE ICMADMIN.ICMSTITEMEVENTS INDEX ICMADMIN.ICMSXITEMEVENTS1X INPLACE  ALLOW WRITE ACCESS  START ;
CONNECT RESET;


CONNECT TO ICMNLSDB;
RUNSTATS ON TABLE ICMADMIN.ICMSTITEMEVENTS ON ALL COLUMNS AND INDEXES ALL ALLOW WRITE ACCESS ;
COMMIT WORK;
CONNECT RESET;
```



Removing log files

It is important to remember to remove log files on a regular basis, as long as they are no longer needed for troubleshooting or audit purposes. This prevents the log files from become overly large, taking up unnecessarily large areas of disk, and becoming unwieldy due to their sheer size. When the log files are removed, they will be recreated by the particular application that created them.

Some log files cannot be deleted while the system is in use because they are being written to. You need to stop the component that is writing to the log file in order to delete it. For a list of log files that you need to regularly check the size of, and if necessary, delete.

It is especially important to remember to check on log files, and remove them when any form of tracing is enabled, as the log files will grow in size much more quickly than usual.

Managing Resource Manager Utilities and services [/etc/rc.cmlsproc & /etc/rc.cmrmproc2]

This section describes a number of utilities and processes that are installed on the Content Manager Resource Manager. The utilities are available on AIX, Linux, Solaris, and Windows. Some of the utilities exist as services on Windows.

For all of the other utilities, you must log on to the server where the Resource Manager is installed. You must log on with a user ID that has DB2 administrative (DBADM) authority.

The utilities and processes include:
The stand-alone application services: RMMigrator, RMPurger, RMReplicator, and RMStager.
The Asynchronous Recovery utilities.
Resource Manager/Library Server validation utility and the Resource Manager Volume validation utility. These two utilities are installed with the Content Manager Resource Manager.

Configuration of Resource Manager Utilities and services

This section provides general background information about configuring Resource Manager Utilities and services.

In Content Manager, there is a central environment setup file, setprocenv.sh for UNIX or setprocenv.bat for Windows. This file stores a set of parameters for each deployed Resource Manager. These parameters are configured automatically when the Resource Manager is deployed and are used by the Resource Manager Services and utilities.

Log configuration settings are specified using the logging and tracing utility in the System Administration Client.

Environment setup file on UNIX includes AIX, Linux, and Solaris.
The following services and utilities depend on one central file, IBMCMROOT/config/setprocenv.sh, for environment setup:

The stand-alone application services: RMMigrator, RMPurger, RMReplicator, and RMStager.
The asynchronous recovery utilities: icmrmdel and icmrmtx
The validation utilities: icmrmlsval and icmrmvolval

The setprocenv.sh file contains one set of environment variables for each Resource Manager.

Environment setup file variables
The following variables are used in the central environment setup file, setprocenv. There is one set of variables for each Resource Manager. Each variable is prefixed with the Resource Manager's identifier.

nodename	**WebSphere Business Integration Server Foundation or WebSphere Application Server nodename.**
was_home	WebSphere Business Integration Server Foundation or WebSphere Application Server home installation directory.
db2home	DB2 instance home directory where the Resource Manager database resides, if the Resource Manager database is a DB2 database.
	On Windows, enter the directory as a fully qualified path with drive letter. For example: C:\Program Files\IBM\SQLLIB.
	On UNIX, enter the directory as a fully qualified path. For example: /home/db2inst1/sqllib. Leave blank if the Resource Manager database is an Oracle database.
db2_jdbc_abspath	If the Resource Manager is using DB2 Type 4 connector, set this to the fully qualified path for the JDBC driver location.
	On Windows, enter the directory as a fully qualified path with drive letter. For example: C:\Program Files\IBM\SQLLIB\java\db2jcc.jar.
	On UNIX, enter the directory as a fully qualified path. For example: /home/db2inst1/sqllib/db2jcc.jar. Leave blank if DB2 Type 4 connector is not in use.
db2_jdbc_license_abspath	If the Resource Manager is using DB2 Type 4 connector, set this to the fully qualified path for the JDBC license file.
	On Windows, enter the directory as a fully qualified path with drive letter. For example: C:\Program Files\IBM\SQLLIB\java\db2jcc_license_cisuz.jar.
	On UNIX, enter the directory as a fully qualified path. For example: /home/db2inst1/sqllib/db2jcc_license_cisuz.jar. Leave blank if DB2 Type 4 connector is not in use.
orahome	Oracle home installation directory, if the Resource Manager database is an Oracle database. Leave blank if the Resource Manager database is a DB2 database.
ora_jdbc_abspath	Fully qualified path for the Oracle JDBC driver location, if the Resource Manager database is an Oracle database. Oracle JDBC 9.0.x is required. Leave blank if the Resource Manager database is a DB2 database.
waittime	Time that the application process main thread waits for the child threads to shutdown before terminating itself.
sleeptime	Time that the client must wait for the process main thread to return an acknowledgement before polling its status again.
CMRM_LOG_DIR	Directory where the log file for the stand-alone application services (RMMigrator, RMPurger, RMStager and RMReplicator) is located.
CMRM_LOG_FILE	Name of the log file for the stand-alone application services (RMMigrator, RMPurger, RMStager and RMReplicator).
initjavaheap	Initial heap size for the stand-alone application services.
maxjavaheap	Maximum heap size for the stand-alone application services.

Resource Manager common utility parameters
In Content Manager, the central environment setup file, setprocenv, contains information about each Resource Manager. This information is used by the Resource Manager Services and utilities. You can, however, override information in the environment setup file by using the following parameters when starting
Services and utilities from the command line.

Configuring the Resource Manager services on UNIX
There are four services: RMMigrator, RMPurger, RMReplicator, and RMStager. In general, the Resource Manager processes are configured using the setprocenv.sh file

However, the values for dbname and rmappname can be changed if passed into the Process starting routine.
These parameters override the ones that are set by the file, $IBMCMROOT/config/setprocenv.sh.

Here is an example of how an entry for the services file appears:
RMMigrator_RMDB 7500/tcp #Resource Manager Migrator

In the example, RMMigrator is the stand-alone application process and RMDB is the database name. The dbname and application parameters passed to the /etc/rc.cmrmproc2 script should match the case in the service name registration in the /etc/services file.

Attention: On AIX, all of the parameters, dbname, rmappname, and application, are case-sensitive. All of the process service names are registered in the /etc/services file.

Starting and stopping resource services on UNIX manually

(NOT supposed to do it on LMS, luckly Livingston never delete records/images from LMS, and also no TSM storage is used for seconday storage purpose)

Anyway, You can start or stop a stand-alone application process as follows:

To start all four applications:

/etc/rc.cmrmprc -act start -db <dbname> -app <rmappname>

Where:

• <dbname> is the database name on which these processes are running.
• <rmappname> is the name of the Resource Manager Web application.

To stop all four applications:

/etc/rc.cmrmproc2 -act stop -db <dbname> -app <rmappname>

To start selective application:

/etc/rc.cmrmproc2 -act start -db <dbname> -app <rmappname> -proc <application>

Where:

• <application> is the Resource Manager stand-alone process you want to start.

For example, to start Resource Manager migrator, RMMigrator, on database rmdb with icmrm as the Resource Manager Web application, use:

/etc/rc.cmrmproc2 -act start -db rmdb -app icmrm -proc RMMigrator

To stop selective application:

/etc/rc.cmrmproc2 -act stop -db <dbname> -app <rmappname> -proc <application>

To start all four applications using the default values for dbname and rmappname, specified in the $IBMCMROOT/config/setprocenv.sh file:

/etc/rc.cmrmproc2 start

Asynchronous Recovery utility

Content Manager includes an automatic scheduled process called the asynchronous recovery utility. The asynchronous recovery runs at the start of each migrator cycle while the migrator is running and enabled and in its runtime window. The migrator should normally be started and enabled. It should only be excluded from running during peak load times.

The purpose is to periodically restore data consistency between a Library Server and its Resource Managers. This process is necessary for the following reasons:

- To provide a rollback function for failed transactions
- To complete scheduled deletion of items that are designated for deletion

The Library Server and Resource Manager can become inconsistent if the Resource Manager is down, or if communication between Information Integrator for Content and Resource Manager fails. The inconsistent state can be reconciled with the asynchronous transaction reconciliation utility. Another important result of running this utility is to clean up known successful transactions. As each creates and update resource item transaction completes, a record is stored in the Library Server database. These records become more numerous and their database table increases in size over time. The table is cleaned up by the transaction reconciliation utility. It is important to run the utility on all of the Content Manager Version 8.1 or later Resource Managers. Also, deleting Resource Manager Resources is an asynchronous activity within Content Manager. When a user uses an application to delete an item, it is deleted, internally, from the Library Server. The asynchronous recovery deletion reconciliation utility is used to mark or physically delete the resource on the Resource Manager.

Resource deletion is a multiple step process. The Resource Manager migrator, running in the background, is responsible for taking all of the resources marked for deletion and physically deleting them. Resource deletion consists of three steps:
An Information Integrator for Content or Content Manager Application deletes an item from the Library Server.
The Asynchronous Recovery Deletion Reconciliation utility marks the resource for deletion on the Resource Manager.

The Resource Manager migrator physically deletes the resource.

Although these processes are scheduled and automatic processes, you might want to run the programs themselves, for example, as part of a database backup procedure. To do so, you need to run two separate utility programs:

The deletion reconciliation utility (**ICMRMDEL**)
The transaction reconciliation utility (**ICMRMTX**)

Attention: Before performing any work, the migrator process will first run the Asynchronous Recovery utilities.
Tip: *In a production environment, synchronize the servers prior to any system backup. This not only ensures that your databases are in a consistent state, but also removes any database entries which represent deleted documents.*

Configuring the Asynchronous Recovery utility

The asynchronous recovery standalone utilities, icmrmdel and icmrmtx, take the common utility parameters and use the default values specified in the environment setup file.

Asynchronous utility logging

By default, the asynchronous utilities log to the console. You can modify the level of information logged and the location of the output in the icmrm_asyncr_logging.xml file. This XML file can be updated to output to FILE if desired. Make sure that the user ID that you use to run the utility has read permission to the XML file, and write permission to whatever log file that you configure for use.

The icmrm_asyncr_logging.xml file is installed with the Resource Manager code in the WebSphere Application Server installedApps path.

On UNIX, the default path to the file is:
/usr/WebSphere/AppServer/installedApps/<nodename>/icmrm.ear/icmrm.war/icmrm_asyncr_logging.xml

Running the Asynchronous Recovery utilities on UNIX

The asynchronous recovery utilities run when you start the migrator. You can also run the asynchronous recovery utilities from a command prompt using two of the common utility parameters. You must be logged in as the root user to run them manually.
To run the deletion reconciliation utility:
Change to the IBMCMROOT/bin directory.
Enter: /icmrmdel.sh -db dbname -app rmappname
To run the transaction reconciliation utility:
Change to the IBMCMROOT/bin directory.
Enter: ./icmrmtx.sh -db dbname -app rmappname

Validation utilities

The purpose of the validation utilities is to analyze discrepancies between three components: the Library Server, the Resource Manager, and the storage system(s) used by the Resource Manager through its defined device managers.

Any of these components can fail and require a restoration via a backup that may be out of synchronization with the other two components.

Because there is no direct link between the Library Server and the storage system, (an example of a storage system is VideoCharger or Tivoli Storage Manager), differences must be reported between the Library Server and the Resource Manager, and the Resource Manager and the storage system using the following utilities:
The Resource Manager/Library Server validation utility (**icmrmlsval.sh** or **icmrmlsval.bat**) generates reports that describe discrepancies between the Library Server and the Resource Manager.
The Resource Manager Volume validation utility (**icmrmvolval.sh** or **icmrmvolval.bat**) generates reports on discrepancies between the Resource Manager and the storage system.

Tip: After running the Asynchronous Recovery utilities, run the **RUNSTATS** function on your databases to ensure that they are operating efficiently

The reports are in XML. You can use commonly available XML tool or browser to view or manipulate the utility output files. Content Manager installs the XML document type definition (DTD) required by the validation utility output files.

You can modify the two utility files with information specific to your Content Manager system. The validation utilities are located in the bin directory in the Resource Manager Installation directory.

The validation utility creates and drops a temporary DB2 table. The environment script requires the resource database name, user ID, password, schema, Web application path, and DB2 instance. To set the environment for both validation utilities, type: **setenvproc.bat** or **setenvproc.sh**.

Validation Logging

By default, the validation utilities log to a file named icmrm.validator.log file in the WebSphere logs directory. You can modify the level of information logged and the location of the output in the icmrm_validator_logging.xml file. Be sure that the user ID that you use to run the utility has read permission to the XML file, and write permission to whatever log file that you configure for use.

The icmrm_validator_logging.xml file is installed with the Resource Manager code in the WebSphere Application Server installedApps path. On AIX, the default path to the file is:
/usr/WebSphere/AppServer/installedApps/<nodename>/icmrm.ear/icmrm.war/icmrm_validator_logging.xml
On Solaris, the default path is:
/opt/WebSphere/AppServer/installedApps/<nodename>/icmrm.ear/icmrm.war/icmrm_validator_logging.xml

Resource Manager/Library Server validation utility

The Resource Manager/Library Server validation utility queries the Library Server for all of the objects created or updated in a specified time period. It then searches the Resource Manager database and detects any discrepancies. The utility runs on the Resource Manager server and requires connectivity to the Library Server database.

To start the utility, navigate to the Resource Manager bin directory and type: **icmrmlsval.sh or icmrmlsval.bat**

The utility creates a temporary table, RMLSITEMS used to accumulate object statistics for the validation. At the end of the validation, this table is normally dropped. If the utility determines that the table is present, it presumes another version of the utility is operating, and exits. If the table is left behind due to an aborted run, you need to drop this table. Connect to the Resource Manager database and drop the table with the following command: **db2 drop table RMLSITEMS**

The following line shows an example of how to invoke the Resource Manager/Library Server utility on an AIX server: **./icmrmlsval.sh -F /reportsdirectory -B 2012-08-30-00.00.00 -E2012-09-01-00.00.00 Parameter Description**

-B *YYYY-MM-DD-HH.MM.SS* The beginning time and date of the objects to examine. Use this parameter with the –E Parameter to restrict the number of objects that the utility must examine. This parameter is optional. If it is not present, all of the objects prior to the -E date are returned, or all of the objects are returned if -E is also not defined.

-E *YYYY-MM-DD-HH.MM.SS* The ending time and date of the objects to synchronize. Use this parameter with the –B Parameter to restrict the number of objects that the utility must examine. This parameter is optional. If it is not present, all of the objects after the -B date are returned, or all of the objects are returned if -B is also not defined.

-F output-path The absolute path to be used for the output files. The utility creates the UTF-8 XML files in this directory. This parameter is required.

-H This parameter displays help information about how to invoke the utility. All other parameters are ignored and no processing occurs.

Resource Manager Volume validation utility

The Resource Manager Volume validation utility checks each object in its database that was added or changed in a specified date range. It queries the device manager for the attributes of that object and generates reports for each object whose information in the database is different than reported by the device Manager. You may want to use the utility if you have a restore data on a volume after a volume crash. The utility helps you to verify that the data is restored correctly. The Resource Manager must be running when you use the utility.

The validation utility does not search the storage system for orphaned objects (objects not referenced by the Resource Manager). Because there are a wide variety of storage systems that are often used for storing files other than those managed by Content Manager, the scanning for orphaned files can be extremely time consuming and may produce a large quantity of false positives.

The Resource Manager volume validation utility runs on the Resource Manager server and only requires access to its own database and the device managers responsible for the volumes that are being checked.

Starting the Resource Manager Volume validation utility

The Resource Manager Volume validation utility is icmrmvolval.sh or icmrmvolval.bat. To start the utility, navigate to the bin directory in the Resource Manager home directory.

The Resource Manager volume validation program uses specific input parameters (see Table 18-3 on page 498). Both dashes (-) and forward slashes (/) are handled as the parameter separator. The parameter tags are supported in both lower and upper case.
Tip: Use the Resource Manager Volume validation utility during times of low traffic on the Resource Manager.

Understanding the validation discrepancy reports

The base file names of the discrepancy reports are “icmrmvolvalYYMMDDHHMMSS_” + Report Type string +”.xml”. The Report Type string identifies the type of discrepancies a report contains. The description of the different report types are detailed later in this section. The timestamp allows the administrator to run the utility multiple times without overwriting the output files. Examples of default names with the default report type are:
cmrmvolval20120531123456_FILENOTFOUND.xml
cmrmvolval20120531123456_SIZEMISMATCH.xml

There are two default discrepancy reports:

Parameter Description
-B *YYYY-MM-DD-HH.MM.SS* The beginning time and date of the objects to examine. Use this parameter with the –E parameter to restrict the number of objects that the utility must examine. This parameter is optional. If it is not present, all of the objects prior to the -E date are returned, or all of the objects are returned if -E is also not defined.

-E *YYYY-MM-DD-HH.MM.SS* The ending time and date of the objects to synchronize. Use this parameter with the –B parameter to restrict the number of objects that the utility must examine. This parameter is optional. If it is not present, all of the objects after the -B date are returned, or all of the objects are returned if -B is also not defined.

-F output-path The absolute path to be used for the output files. The utility creates the UTF-8 XML files in this directory. This parameter is required. If the files currently exist, they are overwritten.

-H This parameter causes the program to display help information about how to invoke the utility. All of the other parameters are ignored and no processing occurs.

-V volume-name The logical volume name on which you want to perform the validation. Use this parameter to limit the number of storage systems to one volume. This parameter is optional. If not used, all storage systems are searched.

File not found Entries are added to the FILENOTFOUND report if an object is in the Resource Manager database, but it is not found on the volume recorded in the database. A file is considered “not found” if the volumes device manager either reports that the file does not exist, or reports that the file has a zero file size when the size in the database is non-zero. The report contains the object information from the Resource Manager database.

Size Mismatch Entries are added to the SIZEMISMATCH report if 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.

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. When updating the Resource Manager volumes, do not run the destager at any point of this process. Otherwise, the volumes will not be the same. Use the following procedures to update the information in the volumes table.

Replacing the staging volume for UNIX

The directory for the staging volume is in the Resource Manager database table, RMSTAGING. Follow these steps to replace the staging volume:
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
If all files in existing staging directory are currently read-writeable, you can skip this step because these files have been destaged already; otherwise, copy all existing files to the new staging volume:
 # cp -rp current_staging_directory new_staging_directory

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:
db2 "connect to <RM db> user <user ID> using <password>"
db2 "update rmstaging set sta_path=staging_path"
Where:

• <RM db> is the Resource Manager database (in our scenario, it is rmdb).
• <user ID> is the user ID (in our scenario, icmadmin) used to connect to the Resource Manager database.
• <password> is the password for the user ID.
• <staging path> is the location of the staging directory, as an absolute path with the trailing slash.

Replacing the storage volume for UNIX

The Resource Manager uses the vol_path + the string_table value of lbosdata + collection + num_bucket_value to develop the path. 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:

Stop the Resource Manager.

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.

Copy all existing files to the new storage volume:

cp -rp current_storage_directory new_storage_directory

Update the location of your storage volume in the Resource Manager database. Use **df -k** to determine the FILESYSTEM and MOUNTED ON location for new storage directory. To update the storage volume, enter the following commands, each on a new line:

db2 "connect to <RM db> user <user ID> using <password>"
db2 "select vol_volumeid,vol_logicalname,vol_mountpoint from rmvolumes"

Where:
• <RM db> is the Resource Manager database (in our scenario, it is rmdb).
• <user ID> is the user ID (in our scenario, icmadmin) used to connect to the Resource Manager database.
• <password> is the password for the user ID.

Determine which VOLUMEID is the one you need to change. For example, to change VOLUMEID=1, the new logical volume is /dev/data1, and mount point is /rm/data1, enter:

db2 "update rmvolumes set vol_logicalname='/dev/data1 'where vol_volumeid=1"
db2 "update rmvolumes set vol_mountpoint='/rm/data1 'where vol_volumeid=1"
db2 "update rmvolumes set vol_size=0 where vol_volumeid=1" db2 "update rmvolumes set vol_path='/rm/data1 'where vol_volumeid=1"
db2 "update rmvolumes set vol_freespace=0 where vol_volumeid=1"

Start the Resource Manager.

Notice that the latter two steps force the Resource Manager to recalculate the volume space and capacity during any new stores. These values are reflected in the RMVOLUMES tables when the Resource Manager shuts down.

Backup

For Content Manager on Multiplatform, it is important to back up five key components:

1. Operation System/Application Software backup: use OS backup tools.
2. The Library Server database: Use db2 TSM database backup tools everyday, db2adutl delete full keep 10 db icmnlsdb without prompting everyday.
3. The Resource Manager database: Use your database manager tools everyday, db2adutl delete full keep 10 db rmdb without prompting everyday.
4. The LBOSDATA directory on every Resource Manager.
5. Tivoli Storage Manager (TSM) volumes.

Jobs	Scripts name	Scheduled by	scheduled running time	logs	Email Distribution
System Backup	ksh -c "/admsrv/admin/bin/sysbkup.ksh rmt0"	root on admsrv1	0:30AM Every Sunday	/admsrv/admin/bin/sysbkup.out	AIXSupport@livingstonintl.com
System Backup	ksh -c "/admsrv/admin/bin/sysbkup.ksh rmt0"	root on admsrv2	1:30AM Every Sunday	/admsrv/admin/bin/sysbkup.out	AIXSupport@livingstonintl.com
DB2 backup	/tsmha1/db2inst1/bin/db2backup.ksh /tsmha1/db2inst2/bin/db2backup.ksh	TSM on admsrv1	23:30PM Every day 23:30PM Every day	/admsrv/drmgr/aix/db2rec01.out.$timestamp /admsrv/drmgr/aix/db2rec02.out.$timestamp	AIXSupport@livingstonintl.com
Retrive FULL DB2 BACKUP Information and Mail to System Admin	/admsrv/drmgr/aix/db2rec01.ksh /admsrv/drmgr/aix/db2rec02.ksh >> /dev/null 2>&1	root	4:50AM Every day 4:50AM Every day	/admsrv/drmgr/aix/db2rec01.out.$timestamp /admsrv/drmgr/aix/db2rec02.out.$timestamp	AIXSupport@livingstonintl.com
Delete expired Full DB2 backup	/admsrv/drmgr/aix/db2del01.ksh /admsrv/drmgr/aix/db2del02.ksh	root	23:30PM Every day 23:30PM Every day	/admsrv/drmgr/aix/db2del01.out.$timestamp /admsrv/drmgr/aix/db2del02.out.$timestamp	AIXSupport@livingstonintl.com
File system Backup (including LBOSDATA)		TSM	Scheduled even in TSM every day		

It is important to remember to back up any data that is migrated to TSM via Content Manager migration policies; otherwise, you will have a single point of failure and data loss within your system. This can be accomplished by using TSM copy storage pools, which may be made up of tape volumes which can be stored off site.

It is not necessary to back up objects within the staging area, as all of the objects within this directory exist elsewhere in the system, and hence already have been backed up if you use the above guideline.

With these five key components, you can rebuild your Content Manager system, even if the original server is completely destroyed. If you choose to back up only the five components listed above (as opposed to a full system backup), you need to reinstall the Content Manager code, and its software prerequisites onto another machine, should the original machine be destroyed, in order to restore your system. Not only should this time taken to reinstall a system be taken into consideration when forming a recovery plan, you must also make sure you have easy access to the installation media, via the original CDs or via a network drive.

If at all possible, perform full backups for each of your Content Manager servers. A hierarchical storage management product such as TSM is ideal for this. When choosing the type of media to back your system up to, consider the relative speed of the media. For example, restoring a DB2 database backup that spans multiple magnetic tapes takes much more time than restoring the same database backup from a fiber attached storage area network (SAN).

TSM is used to back up database backup images and database logs. These backups can be stored on any type of media that TSM supports; therefore, it is possible to back up DB2 archive logs to tape volumes on TSM automatically, reducing the amount of storage space needed on the server running DB2. DB2 can be integrated with TSM so that DB2 commands can be executed as follows:
db2 backup database icmnlsdb use tsm
db2 backup database rmdbls use tsm

Make sure that you back up all components of the Content Manager system together. If you need to restore the system later, each component must be from the same point in time (NOT in LMS).
Identify the LBOSDATA areas. Execute the appropriate query for your operating system:
UNIX: **select vol_mountpoint from rmadmin.rmvolumes**
Pause the system.
Perform the backups. Back up:
Library Server database
Resource Manager database
LBOSDATA areas
Data stored in Tivoli Storage Manager
If possible, before backup database, perform **db2stop**/**db2start** to ensure there are no clients or services connecting to the database in order to perform full backup. Or, for DB2 UDB V8.2 or higher, use quiesce command, for more detailed information about this command.

Resume the system.

Pausing DB2 Content Manager for backups if necessary

(NOT implemented on LMS)

The Library Server PAUSESERVER utility enables you to stop all Content Manager transaction processing in preparation for Library Server and Resource Manager backup processes.

To pause 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 value of MAXTXDURATION. MAXTXDURATION is a column of ICMSTSYSCONTROL table. It is a numeric, which points to the maximum duration by second. 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 Content Manager and leaving you free to create a consistent backup of all Content Manager Servers.

To pause the Library Server, follow these steps:
Open a DB2 command prompt.
Change to the IBMCMROOT\bin directory.
Enter the version of the command for your operating system:
UNIX: ./pauseserver.sh dbname userid password SUSPENDSERVERTIME
Windows: pauseserver.bat dbname userid password SUSPENDSERVERTIME

This command updates the SUSPENDSERVERTIME field in the ICMSTSYSCONTROL 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 ICMSTSYSCONTROL. After that time, all requests to the Library Server are rejected.
For example, if want to pause Content Manager Server on windows platform at 2012-12-14-16:42:00:000000, the local time. The Library Server database is icmnlsdb; userid is icmadmin; password is password, then run below command:
pauseserver icmnlsdb icmadmin password 2012-12-14-16:42:00:000000

Resuming DB2 Content Manager after backups
The RESUMESERVER utility enables you to resume transaction processing.

To resume Content Manager, run RESUMESERVER, which will update SUSPENDSERVERTIME to null and resume transaction processing.

To resume Library Server processing, follow these steps:
Open a DB2 command prompt.
Change to the IBMCMROOT\bin directory.
Enter the version of the command for your operating system:
UNIX: ./resumeserver.sh dbname userid password
Windows: resumeserver.bat dbname userid password

WHTR31147_ admsrv1-bkup

1. File systems (and/or directories/files) to be backup each day, fully or incremental?
   all drives

2. schedule(start time/how long it takes) of each file systems' backup?
   Daily incremental starts at 9pm on : Monday-Tuesday-Wednesday-Thursday-Saturday-Sunday (around 4 hours to complete)
   Full backup starts at 1am on Saturday (around 15h to complete)

3. retention(how long to keep) of each file systems' backup?
   On disks: 35 days (temporary set to 60 days)
   On tapes : Monthly full 390 days – Yearly full 2555 days

WHTR31165_admsrv2-bkup

1. File systems (and/or directories/files) to be backup each day, fully or incremental?

all drives

2. schedule(start time/how long it takes) of each file systems' backup?
   Daily incremental starts at 9pm on : Monday-Tuesday-Wednesday-Thursday-Saturday-Sunday (around 3-4 hours to complete)
   Full backup starts at 1am on Saturday (around 4 hours to complete)

3. retention(how long to keep) of each file systems' backup?
   On disks: 35 days (temporary set to 60 days)
   On tapes : Monthly full 390 days – Yearly full 2555 days