First Editon

IBM Content Manager for Multiplatforms Version 8.1

System Administration Certification Study Guide

John Rodriguez

Bryan Daniel

Lijing Zhang

October 2002

Foreword

In an increasingly competitive marketplace and sometimes uncertain economy, top notch professionals need to be ever vigilant in their pursuit of technical skills. Customers are demanding more complex solutions than ever before, wanting to leverage the company assets they already have. To remain on top, customers need to use data and repurpose in ways never thought possible before. Taking data, in whatever format it exists, wherever the data resides and whenever a customer needs it and putting it to work, is the essence of Enterprise Content Management -- and what this book is all about.

The IBM Content Manager portfolio provides an enterprise content management infrastructure to manage large collections of digital content including text, graphics, images, video, audio and web content. It is designed to easily integrate with customer service, enterprise resource planning, digital asset management and other applications. It can boost the return on information for all types of content across the entire enterprise. IBM Content Manager for Multiplatforms is the industry leading middleware for mission critical applications. The multi-tiered distributed architecture offers scalability to grow from a single department to a geographically dispersed enterprise. The product provides openness to support multiple operating systems, databases, applications and resources, as well as, a secure environment and a single source of access for administration. The XML-ready data model is powerful and expressive. IBM Content Manager provides flexibility and completeness for document management, digital asset management and integrated web content management.

This study guide was put together to help you prepare for the *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* exam and equally important, to help you learn the ins and outs of Content Management from IBM.

A hands-on approach was taken with this study guide. The book takes you through the data model and will walk you through installing the prerequisites for Content Manager for Multiplatforms, including IBM$^{(R)}$ DB2$^{(R)}$ Universal Database and WebSphere Application Server (AEs). The study guide provides screen shots and walks you through the installation of Content Manager step by step. System administration topics are covered in detail. Chapters on troubleshooting and migration are included. You will also see in the appendix a sample *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* exam for you to study.

Content Management is here today and the wave of the future. A Content Management certification will add tremendous value to your technical skills inventory based on the criticality of managing content in both the public and private sectors. Use this study guide to prepare for the certification exam. Keep it as a handy reference as you work with your customers. Your certification will be your road to success in selling and installing IBM Content Management solutions. Best of luck on your exam and your customer endeavors!

Bruce Weed

Manager, IBM Worldwide Content Management Channels Development

Table of Contents

Preface

This book is an excellent way to learn about IBM Content Manager for Multiplatforms Verison 8.1 and to prepare for the *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* exam. Care has been given to cover the areas and topics on the exam, along with providing additional hands-on steps for installing a Content Manager system on a Windows platform. Any Content Manager 8.1 implementation involves a database and web application server. In addition, if content in Content Manager is to be stored on optical, tape, or remote DASD, then Tivoli Storage Manager will be needed in the solution. With this in mind, individuals certified on Content Manager should exhibit knowledge of IBM^(R) DB2^(R) Universal Database, IBM WebSphere Application Server, and IBM Tivoli Storage Manager. If integration with LDAP (Lightweight Directory Access Protocol) is planned, then knowledge of the supported LDAP servers and how they integrate with Content Manager is also needed.

This book is divided into five parts:

- **Part 1 - Introduction to Content Manager (Chapters 1-3)**.
  - **Chapter 1**, An overview of the IBM Content Management solution.
  - **Chapter 2**, Installing the Content Manager prerequisite software products.
  - **Chapter 3**, Installing Content Manager on a Windows platform.
- **Part 2 - System Administration (Chapters 4-8).**
  - **Chapter 4**, The first step in System Administration is reviewing the different options and settings for customizing the Content Manager Library Server and Resource Manager.
  - **Chapter 5,** This is followed by reviewing how Content Manager security works in using privilege sets, access control lists, and administrative domains.
  - **Chapter 6**, The new data model components are reviewed and configured for handling imported data.
  - **Chapter 7,** New document routing support is explained and processes are defined to handle routing imported documents.
  - **Chapter 8**, The IBM^(R) Directory Server Version 4.1 is used to demonstrate the Content Manager LDAP integration. The certification exam does not contain questions on the Directory Server, so if your familiar with one of the other supported LDAP servers then use that to

setup the Content Manager LDAP integration.

- **Part 3 - Object Storage (Chapters 9-11).**
    - **Chapter 9**, Object storage starts with defining the Resource Manager storage components like workstation collections, storage groups, migration policies, and storage systems.
    - **Chapter 10**, If objects are going to be migrated to tape, optical, or backup controlled storage then Tivoli Storage Manager must be used. This Chapter covers the necessary steps for integrating Tivoli Storage Manager with Content Manager. The certification exam does cover the ability to troubleshoot problems with this integration.
    - **Chapter 11**, To complete the object storage area, Content Manager VideoCharger is used to demonstrate how another dedicated resource manager can be configured in Content Manager. Although VideoCharger is not covered in detail on the certification exam, the solution integration aspects are.
- **Part 4 - Content Manager Clients (Chapters 12 and 13).**

  This section will point out the different features of the Content Manager clients while using the access control, data model, and document routing defined in Part 2. The certification exam does contain content covering both clients.

- **Part 5 - Other Considerations (Chapters 14 and 15).**

  This section covers migration of Content Manager from a Content Manager 7.1 Windows platform system to Content Manager Version 8.1. Included in this section is a chapter covering Content Manager troubleshooting topics.

The test objectives and sample test are provided in Appendix A. These should be used as a guide to ensure that you are fully prepared to take the *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* exam. Of course, experience with Content Manager for Multiplatforms Version 8.1 is the best way to prepare for the certification exam. Use this Certification Guide in conjunction with your day-to-day use of Content Manager to assist you in preparing for the exam.

The *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* exam tests skills in the following areas:

- Knowledge of the IBM Content Management solution
- Ability to implement the appropriate system to meet requirements
- Installing and configuring Content Manager
- Defining the data model to meet customer requirements
- Text indexing of data
- Setting up Content Manager security
- Managing users and groups including LDAP integration
- Defining document routing
- Setting up object storage including Tivoli Storage Manager
- Content Manager migration
- Troubleshooting, including integration issues with Tivoli Storage Manager and application performance options with IBM(R) DB2(R) Universal Database.
- Content Manager clients (what features are supported)
- Migration

Because Content Manager is highly integrated with IBM(R) DB2(R) Universal Database, it is recommended that individuals desiring to be certified on Content Manager also consider a DB2 certification. Two exams would be beneficial: *DB2 Family Fundamentals (512)* and *DB2 for OS/2, Windows, UNIX, and Linux Database Adminstration (513)*. In addition, certification on Tivoli Storage Manager would greatly assist in troubleshooting the object migration issues between the products; *IBM Tivoli Storage Manager V5.1 Implementation (772)*.

Note: More information about IBM certifications can be found at http://www.ibm.com/certify.

Conventions

Each chapter provides hands-on steps for performing the steps necessary to work through the topics on an actual system. Included are many screen shots of the system. The intent is not to include all screens shots from an area, but only those that are necessary to represent the actions being taken. All figure and table references should be referred to in the text covering the particular topic.

Some examples might be included in a shaded box. Items included would be configuration file examples, SQL Commands, error log text, and any other item that would come from a system source file.

```
SELECT tracelevel
FROM ICMSTSYSCONTROL
```

Occasionally, notes are provided to highlight a particular point or feature of Content Manager or the integrated topic being covered. Special attention should be given to the highlighted notes.

Note: May be used to highlight items of importance that may have also existed in previous releases of Content Manager.

Note: May be used to highlight important concepts and features new to Content Manager 8.1. Or point out a particular step relevant to what might be covered on the certification exam.

To emphasize a term or concept, the term is shown in *italics*. To highlight an action or important step to be taken the term, action, or text is shown with a **bold** type.

Contributions

This first edition of *Content Manager Version 8.1 Certification Guide* has been prepared by the authors based on experience with Content Manager and the knowledge gained while supporting Business Partners that participated in the Content Manager Version 8.1 beta program. Of course with any new release of a software product, the initial core knowledge of a product's function and features comes from the architects and developers who labored long hours to make the product a reality. Because of their efforts to build the product, provide early training at the beginning of the beta, training as the product neared general availability, and patience while everyone else discovered their invention, we all benefit by having a new product to sell and support. So many thanks to the IBM Content Management Development Team located at the IBM Silicon Valley Laboratory in San Jose, California.

In addition there are others to thank:

- **Mike Adair**, Software Engineer for IBM PartnerWorld for Developers Technical Support, for taking the extra time to review and comment on this guide.
- **Mike Langer**, Software Engineer for IBM PartnerWorld for Developers Technical Support, for reviewing this guide and stepping through many of the exercises to verify the requested steps.
- **Darren Marshall**, Software Engineer on contract with IBM PartnerWorld for Developers Technical Support, for reviewing this guide and stepping through many of the exercises to verify the requested steps.
- **Bruce Weed**, Manager IBM Worldwide Content Management Channels Development, for arranging the resources to allow this guide to be developed.
- **Jacqueline Ichniowski**, Content Management Channels Development, for her constant encouragement, faith, and trust while the certification exam and study guide were being developed.
- **Cathy McCluney**, Manager IBM PartnerWorld for Developers Technical Support Data Management, for allowing the Content Management support resources to be used in working on the certification exam and this study guide.
- **Bob Shipione**, editor on contract with IBM PartnerWorld for Developers Technical Support, for providing tool expertise and editing guidance while the guide was developed.

Special thanks to Wendy Rodriguez who assisted with this project providing a keen eye to flush out grammatical and formatting problems.

Authors

Bryan Daniel

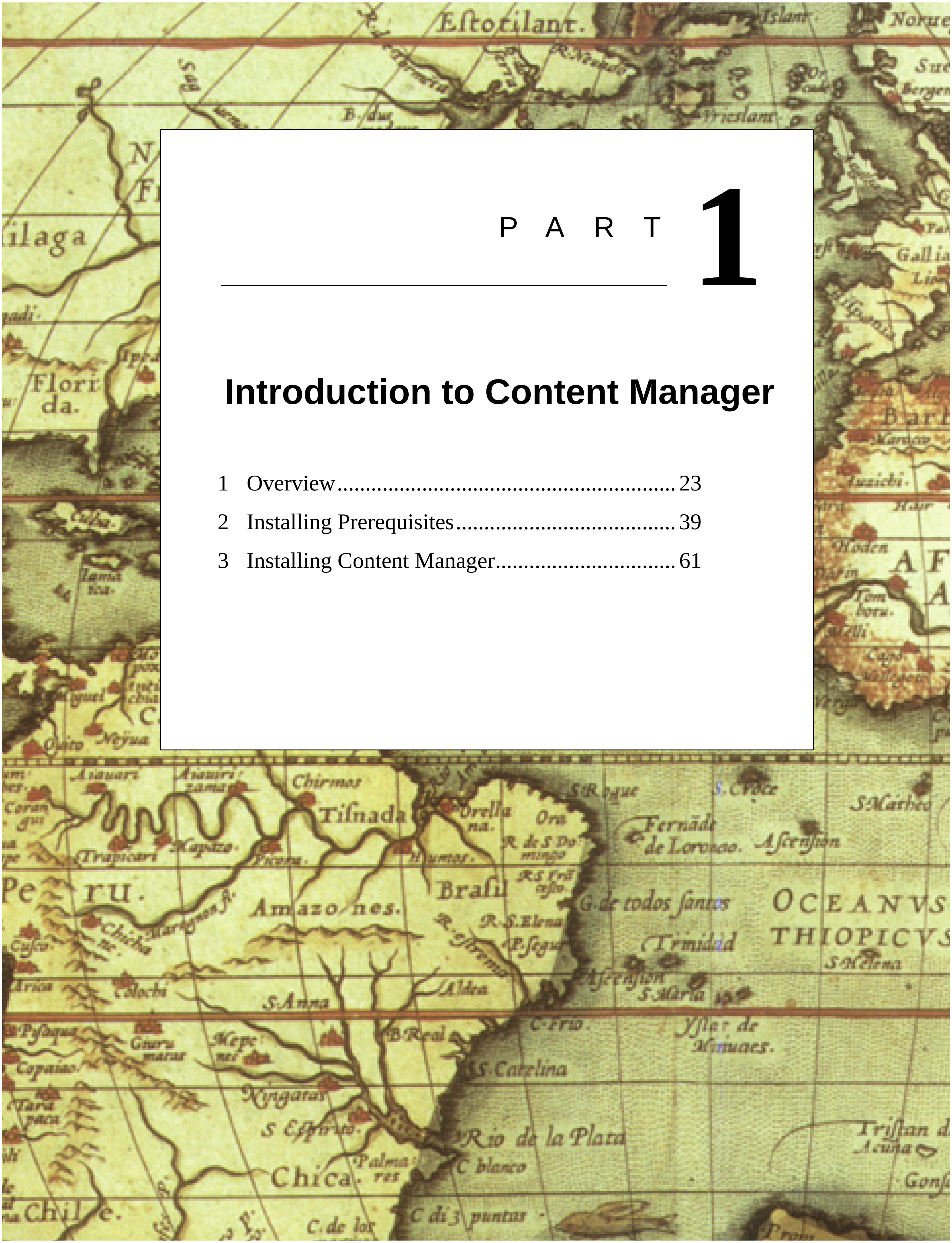
Bryan Daniel joined the IBM Corporation as a Software Engineer in 1999 after graduating from Florida International University with a Bachelor's of Science in Computer Engineering. Bryan currently provides IBM Content Management support to the business Business Partner community, with a focus on IBM Content Manager for Multiplatforms, IBM Enterprise Information Portal, and Content Manager eClient. Bryan's certifications include *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* and *Certified Solutions Expert (CSE) - IBM Content Manager - OnDemand Multiplatform (440)*. Bryan Daniel can be reached at bryand@us.ibm.com.

John A. Rodriguez

John Rodriguez has been with the IBM Corporation for over eighteen years with various responsibilities in software development and Business Partner support. John is currently the team lead for the IBM PartnerWorld for Developers Content Management Technical Support (Developer Technical Support Center - Dallas) providing support for IBM Content Manager for Multiplatforms and IBM Enterprise Information Portal. John's certifications include *IBM Certified Solutions Expert (CSE)* - *IBM Content Manager Version 8 (442)* and *Certified Solutions Expert (CSE)* - *IBM Content Manager* - *OnDemand Multiplatform (440)*. To reach John Rodriguez, please send mail to johnarod@us.ibm.com.

Lijing Zhang

Lijing Zhang joined the IBM Corporation as a Software Engineer in 2001 after multiple software engineering contract experiences. Lijing currently provides IBM Content Management support to the business Business Partner community, with a focus on IBM Content Manager for Multiplatforms, IBM Enterprise Information Portal, and IBM Content Manager VideoCharger. Lijing's certifications include *IBM Certified Solutions Expert (CSE)* - *IBM Content Manager Version 8 (442)* and *Certified Solutions Expert (CSE)* - *IBM Content Manager* - *OnDemand Multiplatform (440)*. To reach Lijing Zhang, please send mail to lijing@us.ibm.com.



PART 1

Introduction to Content Manager

CHAPTER 1

Overview

- Enterprise Content Management
- Content Manager
- Enterprise Information Portal
- Content Manager for Multiplatforms

This chapter will introduce the IBM Enterprise Content Management Portfolio and the applications that comprise that portfolio. An overview of IBM Content Manager and Enterprise Information Portal is provided. The different components of the IBM Content Manager for Multiplatforms system will be reviewed. An overview of Content Manager's new data model and document routing will be provided. The new Content Manager eClient will be introduced, along with, the re-architecture of the Content Manager servers to facilitate greater performance and flexibility for supporting integrated solutions.

Enterprise Content Management

IBM *Content Manager* is a centerpiece of IBM's Enterprise Content Management offering that provides an out of the box content management solution including an integrated platform for e-business solutions. Built on the strength and flexibility of IBM(R) DB2(R) Universal Database, Content Manager crosses operating system platforms to provide integrated solutions a solid and secure base for storing and managing large quantities of multimedia content. This content includes documents, images, audio files, streaming video, billing reports, business records, and object content needed for web content management solutions. Solutions for Web Content Management, Media Advertisement, Enterprise Resource Management (ERP), Customer Relationship Management (CRM), Supply Chain Management (SCM), and many others benefit from Content Manager's ability to manage and archive data and object content.

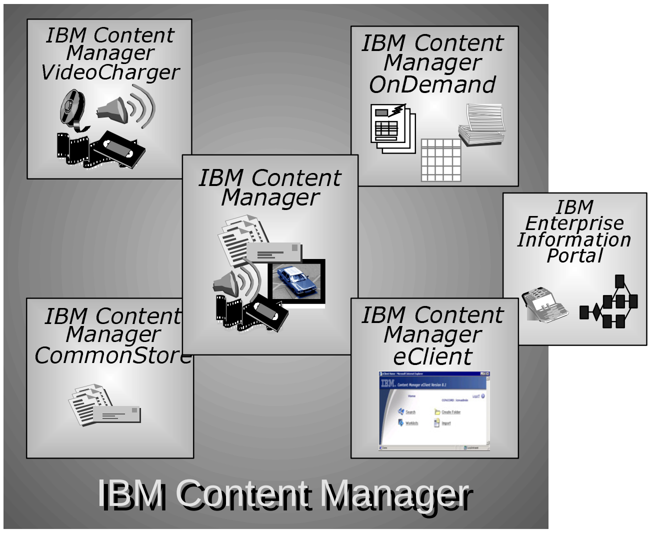

IBM Content Manager VideoCharger
IBM Content Manager OnDemand
IBM Content Manager
IBM Enterprise Information Portal
IBM Content Manager CommonStore
IBM Content Manager eClient
IBM Content Manager

Figure 1–1 *IBM Enterprise Content Management Portfolio*

To provide a rich content object datastore the Content Manager solution consists of the overall object management system named Content Manager and specialized servers to handle specific content seen in Figure 1–1. IBM Content Manager VideoCharger is an example of a specific server designed to handle the large streaming video files. VideoCharger integrates with the Content Manager product to off-load the storage, archival, and delivery of videos. IBM Content Manager OnDemand was designed to store print spool files and billing reports which generate database indexed data for fast query and retrieval based on the content of the files and reports stored in OnDemand. IBM Content Manager OnDemand also provides the added feature of being able to store and manage different document formats for companies requiring object management along with their reporting system. IBM Content Manager CommonStore provides an archival bridge between the datastores of IBM Lotus Domino, Microsoft Exchange and SAP R/3, to the Content Manager server or Content Manager OnDemand. The mail, documents, and data Commonstore moves to Content Manager can still be accessed from within the original application using Commonstore.

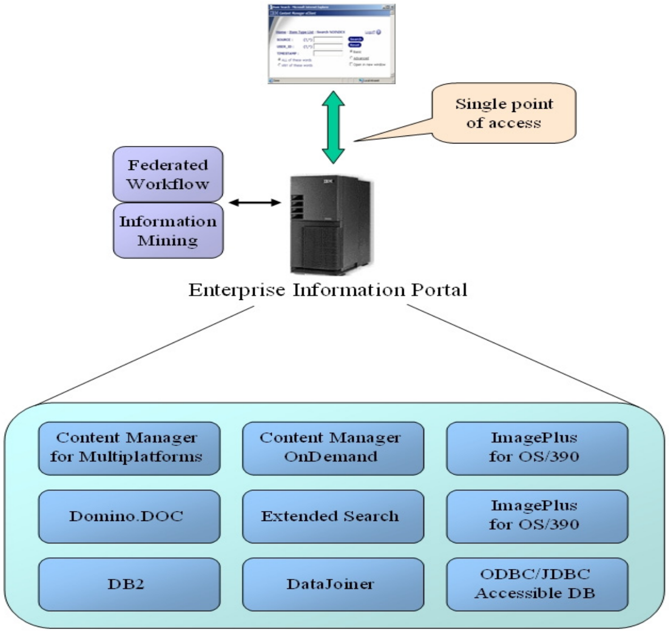


Figure 1–2 *Enterprise Information Portal information integration*

To facilitate the implementation of services for Enterprise Content Management, Enterprise Information Portal provides the information integration toolkits and other options required for solutions to connect to the various Content Manager servers. Enterprise Information Portal or EIP consists of integration connectors that understand how to access the information stored in different back-end servers and deliver that information through a federated interface for applications or client solutions (Figure 1–2). The toolkit provides connectors in C++ and Java including a Java Bean interface for use in building solutions on the Content Manager platforms. EIP uses query templates stored in a database so customers can map metadata and other referential information from the back-end servers to the information attributes the customer wants presented to their users. EIP also includes services like Information Mining and Advanced Workflow for gathering, correlating, and processing information gathered from the data sources that EIP can connect to.

The EIP connectors provide the connection used by the Content Manager eClient web application. Content Manager eClient is a browser based client providing support for accessing the content stored in Content Manager and Content Manager OnDemand. When used with these back-end servers, the eClient presents a document management based style for importing, retrieving, and handling delivered content.

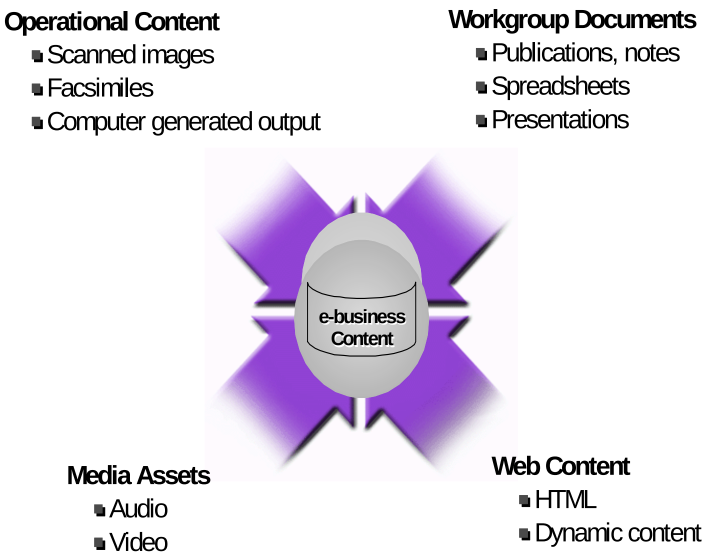


Figure 1–3 *Content Manager the repository for e-business solutions*

Content Manager combined with Enterprise Information Portal provide the repository and integration services required by integrated applications for the capture, creation, organization, workflow, archival, and life cycle management of today’s complex media based solutions (Figure 1–3). Together they provide a consistent information model with transaction, security, process integration, and life cycle services which allows content solutions to focus on delivering the right information to the right people.

Content Manager for Multiplatforms

The *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* exam covers the new version of Content Manager for Multiplatforms. This version is composed of the Content Manager server and clients that currently operate on the Microsoft Windows and UNIX platforms (IBM AIX and Sun Solaris). The exam does not contain specific content concerning the IBM Content Manager for iSeries or the Content Manager ImagePlus solution running on the IBM zSeries platform. Experience with earlier releases of IBM Content Manager for Multiplatforms will help in taking the test, however, the content on the test is centered around Content Manager for Multiplatforms Version 8.1 where some of the concepts such as the data model and server architecture have changed. So the remaining information in this section will pertain to Content Manager 8.1.

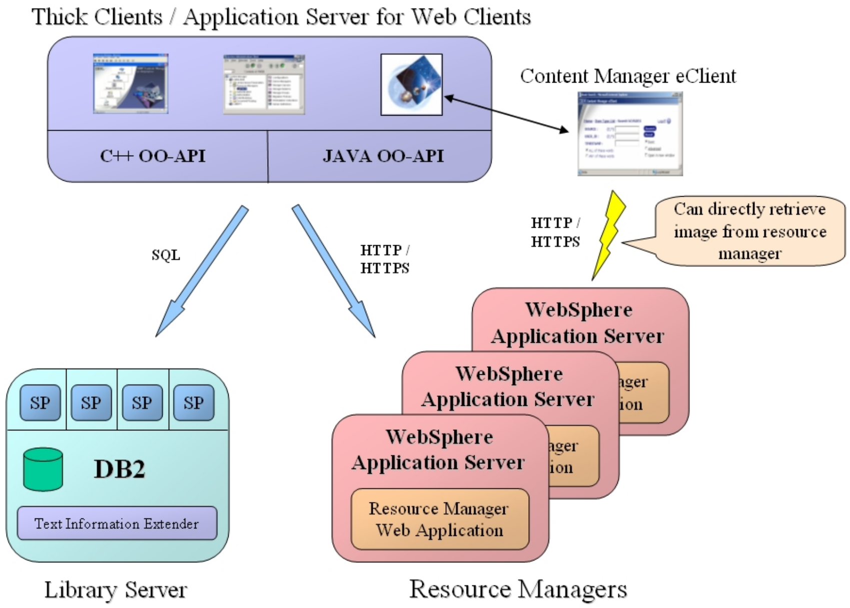

Thick Clients / Application Server for Web Clients
C++ OO-API
JAVA OO-API
Content Manager eClient
SQL
HTTP / HTTPS
HTTP / HTTPS
Can directly retrieve image from resource manager
WebSphere Application Server
WebSphere Application Server
WebSphere Application Server
Resource Manager Web Application
SP
SP
SP
SP
DB2
Text Information Extender
Library Server
Resource Managers

Figure 1–4 *Content Manager for Multiplatforms version 8.1*

Content Manager for Multiplatforms continues to provide an architecture consisting of a Library Server, a server to store imported objects, clients demonstrating a document management model, and a rich set of Application Programming Interfaces (APIs). As Figure 1–4 demonstrates, the pyramid architecture of Content Manager for Multiplatforms resembles previous releases, however, each of the components have undergone major changes. In Content Manager version 8.1 a system implementation continues to consist of a single Library Server, multiple Resource Managers (formerly called an Object Server), and clients or line of business applications. Even though multiple Library Servers can be installed on a single computer, the naming of the database represents the Library Server for that particular Content Manager system.

The Library Server is a database application that manages user profiles, access control, document routing procedures, and the object metadata defined by the new data model definition in Content Manager. Associated with a Library Server are multiple Resource Managers to manage the object content. The main Resource Manager is a web application running on IBM WebSphere Application Server. Content Manager Video Charger is also a Resource Manager designated to handle the large video stream files stored in Content Manager.

The Content Manager clients or integrated solutions make the initial connection to the Library Server for authorization to access the system. Once access and connection have been provided, the users or solutions are granted specific privileges assigned in the privilege set for their profile. While connected, templates, called item types, are used to define, import, query, and retrieve objects in the system. All activities other than storing the actual object are performed against the Library Server. When users store or retrieve objects into the system the client application or integrated solution works directly with the Resource Manager assigned to that user for the actual processing of the object. The object or file does not flow through the Content Manager Library Server.

The benefits this model provides include:

- The separation of information defining the content stored between the Library Server and Resource Managers.
- A new item type data model provides greater flexibility in defining the model used to represent content stored in the system.
- Greater performance as all queries are executed against the Library Server which benefits from the performance of the underlying database.
- Better performance as the storage and retrieval of objects is handled between the client solution and the Resource Manager freeing up the Library Server.
- Support for multiple distributed resource managers for storing digital objects close to the users who need to access them frequently.

Library Server

The Library Server is the key component of the Content Manager system and is built on IBM(R) DB2(R) Universal Database using stored procedures (Figure 1–5). Access to the Library Server is through the database query language SQL. At a minimum, this access requires the client workstations to run the DB2 Runtime Facility. The client workstations perform queries against the Library Server and are passed tokens (locators for the requested object content) pointing to the Resource Manager containing the desired object or file. The client uses the token to communicate directly with the Resource Manager where the object is transferred to the client using standard Internet protocols like (HTTP, FTP and File).

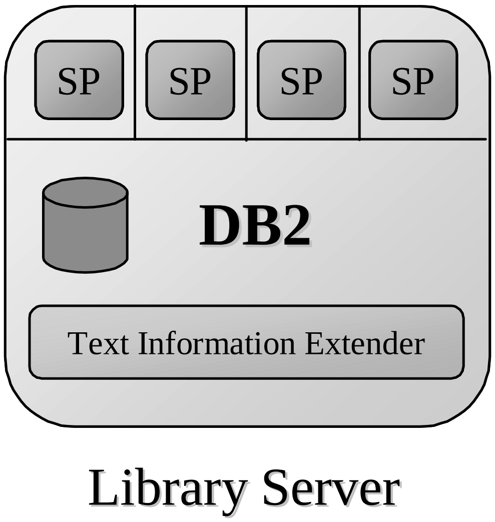


Figure 1–5 *Content Manager Library Server architecture*

In addition, Content Manager includes DB2 Text Information Extender (TIE) which allows for full text searching of documents in the Content Manager (Figure 1–5). The Library Server controls the connection to TIE and determines through the item type template definition and the media object type which objects will have their text content indexed.

The main responsibilities of the Library Server include user management, system access authorization, object access authentication, storing metadata defined by the system data model definition, and managing the Content Manager document routing process. These functions are represented in the

Content Manager System Administration Client as Authentication, Authorization, Data Modeling, and Document Routing. Each of these is covered in detail in later chapters of this study guide.

Authentication

The Library Server defines the users and user groups that can access the Content Manager System. Those users and groups can reside in an LDAP directory. The Library Server provides support for connecting to the LDAP server importing user and group definitions. Added to Content Manager Version 8.1 is the concept of Administrative Domains. Domains allow the Content Manager system to be viewed as different subsystems from an administrative level. The main System Administrator can initiate Administrative Domains and define different domains for various operating units of a business. Administrators in those operating units are then granted the authorization to create, manage, and delete users in their domains.

Users and user groups are described in greater detail in *Chapter 5 Managing System Access* of this study guide. LDAP integration is cover in detail in *Chapter 8 LDAP Integration* of this study guide.

Authorization

The Library Server provides support for authenticating who can access the system, defined data model templates, and object content stored on a Resource Manager. To accomplish this, the Library Server uses privileges assigned to user profiles and Access Control Lists (ACLs) that grant access to stored objects. When users are defined to Content Manager, they are assigned a privilege set which is a group of privileges. This privilege set defines the maximum rights the user has for working with the Content Manager system. Privilege sets are also used to match users and groups to a set of privileges granted for all object content stored in Content Manager. These ACLs specify the maximum rights that can be exerted against a specific object in the system. The ACL cannot grant the user more rights that what they already have defined in their user profile, but can restrict the rights the user already has to a more limited set of actions for a specific object.

Privilege sets, privileges and Access Control Lists are described in greater detail in *Chapter 5 Managing System Access* of this study guide.

Data Modeling

Objects stored in Content Manager are represented as items. Items are defined by an item template called an Item Type. Item Types provide support for defining a detailed hierarchical data model allowing a single root component for each item and multiple child components or object definitions for each item root component (Figure 1–6).

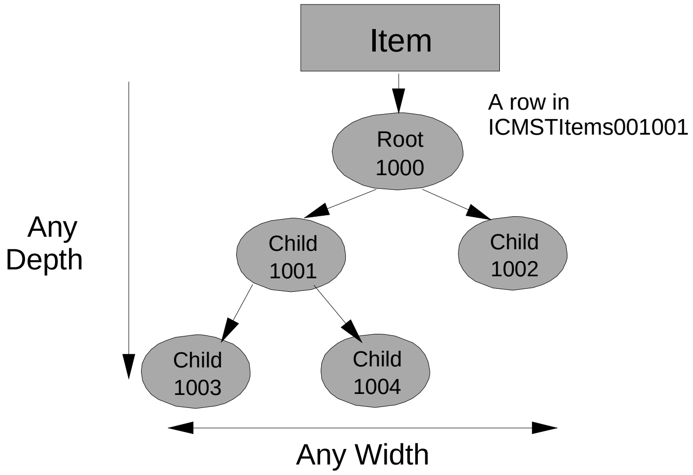


Figure 1–6 *Content Manager Item Type definition Model*

The Content Manager item type provides the template for assigning attributes that will describe the stored object, the classification that will define the type of item being created, and the access control list for the stored item. Content Manager by default recognizes four different item type classifications: item, resource, document, and document part. *Items* represent definitions in the Library Server database where there are no parts or object files stored in the Content Manager Resource Manager. *Resource* represents objects of different media type definitions stored on the Resource Manager that are normally linked to different data components of integrated solutions. *Document* is a model use in Content Manager to represent an Enterprise Content or Document Management system. The

Document item type provides the base Resource Manager parts required by the Content Manager clients to store documents, images, and other files, along with annotations and notelogs. A document base part also can be used to indicated objects whose content needs to be indexed. *Document part* is used to define additional document management parts that can be used in the document item type model.

The Content Manager item type definition will also allow the attributes in the item type to be linked as a Foreign Key to attributes residing in another item type or in a database table column outside of the Content Manager database. Auto-linking within the item type provides a way to have imported objects automatically referenced by another item type. It also provides the mechanism for auto-foldering within the Content Manager solution.

The Content Manager data model is covered in detail in *Chapter 6 Defining the Data Model* of this study guide.

Document Routing

Document routing in Content Manager is a workflow definition contained within the Library Server. It provides a means for defining a basic workflow process for moving documents and folders through a number of work nodes. Actions taken by users and integrated solutions determine whether the folder or document continues to move down the process or is routed through another process (Figure 1–7).

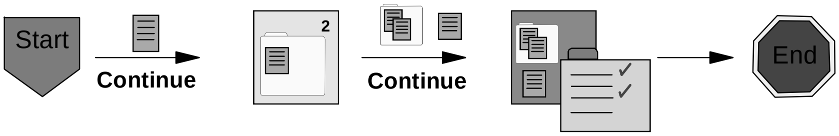


Figure 1–7 *Content Manager document routing process*

The Content Manager clients support the worklist definitions for document routing which provide users access to the documents and folders residing on the different document routing work nodes. This provides users access to the items being handled within a process.

Content Manager Document Routing is described in detail in *Chapter 7 Building Document Routing* of this study guide.

Resource Manager

The Resource Manager is a web application that can be installed on the same workstation as the Library Server or on its own machine. The Resource Manager runs on IBM WebSphere Application Server, utilizing the database capabilities of IBM(R) DB2(R) Universal Database.

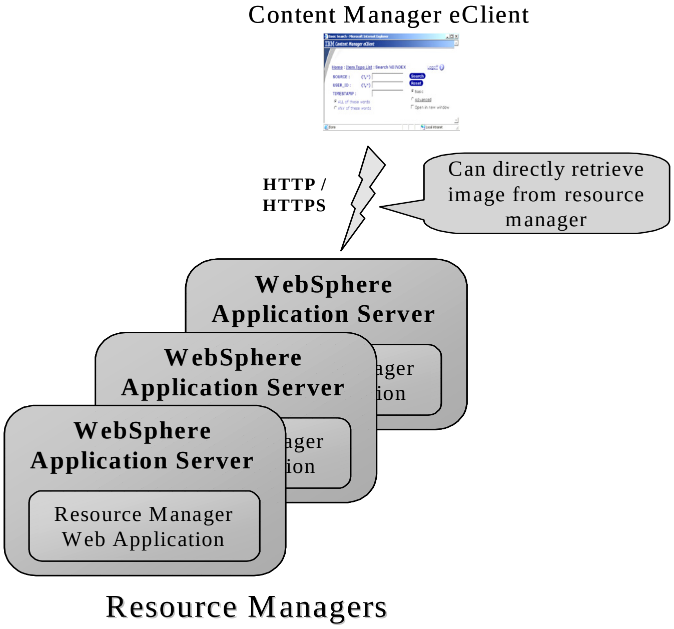

Content Manager eClient
HTTP / HTTPS
Can directly retrieve image from resource manager
WebSphere Application Server
WebSphere Application Server
WebSphere Application Server
Resource Manager Web Application
Resource Managers

Figure 1–8 *Content Manager Resource Manager*

The Resource Manager is the repository for objects stored in the Content Manager system. Solutions or Content Manager clients query the Library Server and retrieve a hit list of items in the system. When the clients request an object, the Library Server provides a token to the client indicating the location of the object on a designated Resource Manager. The client or solution then uses the token to do a direct retrieval of the object from the Resource Manager (Figure 1–8).

Note: A single Library Server can support multiple Resource Managers with object content can be stored on any of them.

Content Manager also utilizes the service of IBM Tivoli Storage Manager for migrating object content to archival datastores. These definitions are defined in the Content Manager Resource Manager.

The Content Manager Resource Manager is defined in *Chapter 9 Resource Manager* of this study guide. The procedures for integrating IBM Tivoli Storage Manager with Content Manager are contained in *Chapter 10 Tivoli Storage Manager* of this study guide.

System Administration Client

The Content Manager System Administration Client is used to manage the Content Manager System and define the following features:

- Defining your Data Model
- Configuring Library Servers
- Configuring Resource Managers
- Defining Users and Access Control
- Defining Document Routing
- System Managed Storage

Details for the System Administration Client are described in detail throughout this study guide as each topic is covered. The System Administration Client can be used to manage both Content Manager and Enterprise Information Portal databases.

Content Manager Clients

Client for Windows

The Content Manager Client for Windows provides both import and scan support for Content Manager. Users can issue queries using the item type templates to locate documents and folders stored in Content Manager. The Client for Windows uses the Content Manager connector defined in EIP for connecting to Content Manager.

The Content Manager Client for Windows is described in detail in *Chapter 12 Client for Windows* of this study guide.

eClient

The Content Manager eClient uses the EIP connector for Content Manager to access the services of Content Manager. The eClient provides a web browser based client for working with content stored in Content Manager.

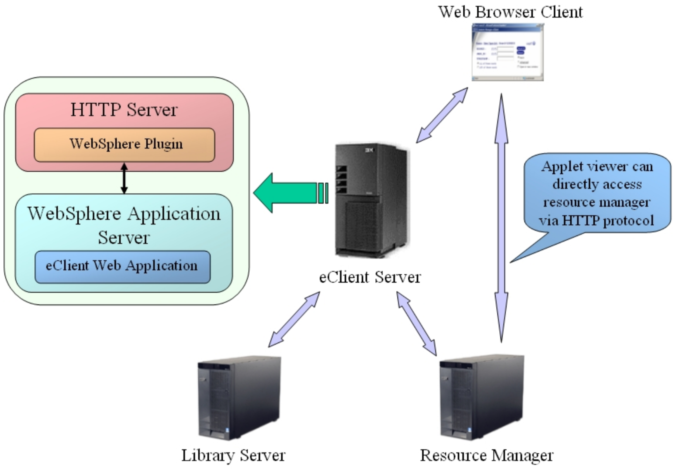


Figure 1–9 *Content Manager eClient*

Content Manager eClient version 8.1 provides a significant enhancement in the way documents and images are rendered and delivered to the browser client (Figure 1–9). With the new design, items selected in the search results hit list can be retrieved directly from the Content Manager Resource Manager if the new Viewer Applet is being used. The Viewer Applet interacts directly with the Resource Manager to retrieve the desired object and then handles the rendering of the object as users perform actions on the displayed object.

The Content Manager eClient is described in detail in *Chapter 13 eClient* of this study guide.

Start Here CD

The Start Here CD is an important part of the IBM Content Manager installation package and is designed to provide a single access point for product packaging, planning information, and installation assistance using an interactive planning wizard. Insert the Start Here CD into a machine and the CD launches automatically providing a very good overview and introduction of Content Manager.

Information Center

The Information Center (Figure 1–10) is a Java / HTML based, searchable version of the Content Manager documentation library. The Information Center has the following on-line documentation:

Content Manager

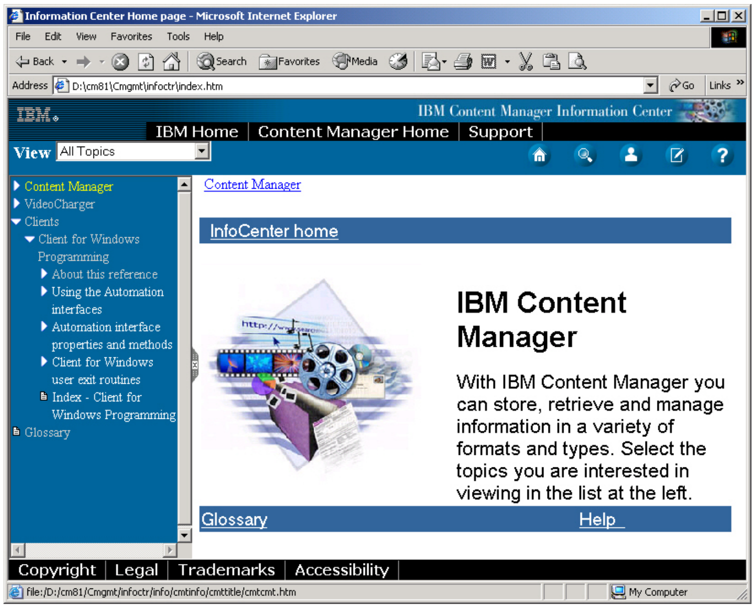
- Planning and Install
- Administration
- Migration
- Trouble Shooting

VideoCharger

- Planning and Install
- Administration
- Programming

Clients

- Client for Windows Programming



Address D:\cm81\Cmgmt\infoctr\index.htm

View All Topics

IBM Content Manager

With IBM Content Manager you can store, retrieve and manage information in a variety of formats and types. Select the topics you are interested in viewing in the list at the left.

file:/D:/cm81/Cmgmt/infoctr/info/cmtinfo/cmttitle/cmtcmt.htm

Information Center Home page - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Go
Links
IBM.
IBM Content Manager Information Center
IBM Home
Content Manager Home
Support
Content Manager
VideoCharger
Clients
Client for Windows Programming
About this reference
Using the Automation interfaces
Automation interface properties and methods
Client for Windows user exit routines
Index - Client for Windows Programming
Glossary
Content Manager
InfoCenter home
Glossary
Help
Copyright
Legal
Trademarks
Accessibility
My Computer

Figure 1–10 *Content Manager Information Center*

The eClient on-line information (Installing, Configuring, and Managing eClient) is installed as a separate on-line reference when eClient is installed on the server.

Table 3-1 lists the manuals for Content Manager for Multiplatforms, Enterprise Information Portal, and VideoCharger that should be used for the official description of the Content Manager features.

Table 3-1 *Content Manager Documentation Library*

Number	Title
	Content Manager
GC27-1332	Planning and Installing Your Content Management System
SC27-1335	System Administration Guide
SC27-1343	Migrating to Content Manager Version 8
SC27-1350	Installing, Configuring, and Managing the eClient
	Common to all
SC27-1347	Workstation Application Programming Guide
SC27-1349	Messages and Codes
	Enterprise Information Portal
GC27-1345	Planning and Installing Enterprise Information Portal
GC27-1364	Installing IBM Content Manager for Panagon Image Services
SC27-1346	Managing Enterprise Information Portal
	VideoCharger
GC27-1353	Planning and Installing VideoCharger
SC27-1351	Administrator’s Guide and Reference
SC27-1352	Programmer’s Reference

Summary

Content Manager provides a flexible secure content management system that can be used for Enterprise Document and Imaging Management. Using the API connector toolkit provided with Enterprise Information Portal, all kinds of solutions can be integrated with Content Manager to take advantage of the strong object management facilities. The chapters that follow will walk you through the features of Content Manager. Using this guide along with the actual Content Manager software is the preferred method for learning the product and studying for the exam.

This study guide attempts to provide a practical hands-on reference to assist in learning Content Manager and prepare for the *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* exam. It is not the intent of this guide to replace the information provided in the Content Manager Documentation Library or on-line help system. Use this guide as an added source of information.

CHAPTER 2

Installing Prerequisites

- DB2 Universal Database
- DB2 Text Information Extender
- WebSphere Application Server
- Microsoft Visual C++ Compiler
- Tivoli Storage Manager
- LDAP Server

In this chapter you will review the prerequisite software required by Content Manager on Windows. Troubleshooting tips are also provided in case of difficulty.

An installation procedure is woven into this chapter to provide an exercise demonstrating how to install the prerequisite software for Content Manager Version 8.1. To use the integrated exercise, simply follow the numbered procedures.

The exercises in this chapter are divided into the following sections:

- Install DB2 UDB v7.2
- Install DB2 Text Information Extender v7.2 (TIE) + Fixpak 1
- Install DB2 UDB v7.2 Special Fixpak 7 For CM
- Install WebSphere Application Server AEs v4.0 + PTF3
- Install Microsoft Visual C++ v6.0
- Configure environment variables

Hardware Requirements

Before installing any software, be sure that the workstation meets the hardware requirements for both Content Manager and the prerequisite software. A detailed listing of the Content Manager hardware requirements can be found in the publication entitled *Planning and Installing Your Content Management System* (GC27-1332). For the hardware requirements of the prerequisite software, please see the installation guides supplied with each software package.

Requirements for Exercises

The exercises throughout this study guide walk you through the process of installing and configuring a Content Management system on a **single** Windows machine. In this chapter, you will install the prerequisite software needed by the Content Manager servers. In order to complete the exercises in this guide, your workstation should meet the hardware requirements shown in Table 2–1.

Table 2–1 *Hardware Requirements*

Component	Required
CPU	Intel Pentium 800 MHz or equivalent
RAM	512MB absolute minimum (only Content Manager related software could be running) 1 GB recommended
Storage	3 GB of free space
Display	SVGA (800x600 resolution and 256 colors)
Other Required Hardware	Mouse CDROM Drive (for installation) Network adapter that has a TCP/IP address (if you donÕt have a network adapter, install the Microsoft Loopback adapter)

Note: These requirements are for the purpose of setting up a test system, and do not necessarily reflect production requirements.

Installing Prerequisites on Windows

This section provides an overview of the prerequisites needed in order to install the following Content Manager components on the Windows platform:

- Library Server
- Resource Manager
- System Administration Client
- Information Center

Before You Begin

Before you begin the software installation:

1. ___ Make sure you have a user ID that will be used to perform the installation and meets the following conditions:

- Belongs to the Local Administrator's group
- One to eight characters in length.

Notes:
1. It is very important that you do not use the default user ID of **Administrator**. This user ID is more than eight characters, and will cause the Content Manager database creation scripts to fail.

2. User IDs must also follow the rules outlined by the relational database manager you are using.

For the purpose of the exercises contained in this study guide, it is recommended that you create an administrative user ID called **admin** and use this ID to perform the software installation and configuration.

2. ___ If the Enterprise Information Portal has ever been installed on this workstation, you need to remove the following environment variable from the workstation:

```
DB2_STPROC_ALLOW_LOCAL_FENCED =1
```

IBM DB2 Universal Database

IBM(R) DB2(R) Universal Database V7.2 is required for the Library Server and the Resource Manager.

Note: When used with Content Manager Version 8,1, DB2 V7.2 requires DB2 Special Fixpack 7 for Content Manager.

Special Fixpack 7 (FP7) can be downloaded from the following location:

http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/fp7_cm.d2w/report

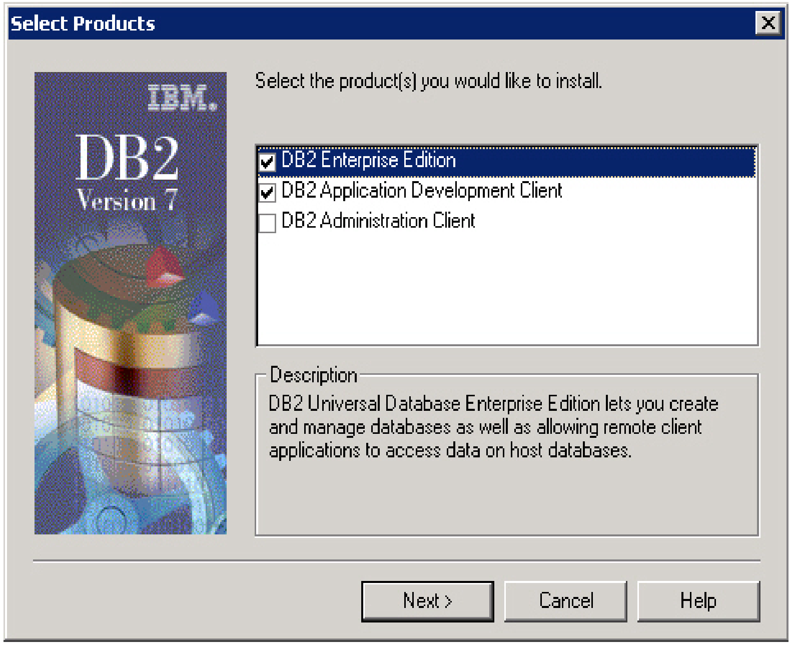
All Content Manager servers store their data in a database. By default, the database names are *ICMNLSDB* (Library Server) and *RMDB* (Resource Manager). This not only allows Content Manager to store and retrieve information efficiently, but also allows the servers to leverage some functionality of the database manager (for example, indexes, tablespaces, views, etc.). The DB2 Application Development Client (a selectable component during the DB2 UDB installation) is also required by the Library Server and the Content Manager System Administration Client.

The chapter, *Installing Prerequisites*, in the publication entitled *Planning and Installing Your Content Management System* (GC27-1332) provides detailed instructions for installing DB2 UDB on the various operating system platforms.

Note: The DB2 UDB Fixpak should always be installed (or reinstalled) after installing either DB2 TIE or any DB2 TIE Fixpaks. This will ensure that the DB2 UDB files are at proper levels.

The following exercise provides instructions for installing DB2 UDB V7.2 on your Windows workstation.

1. ___ Insert the DB2 UDB V7.2 CD into your CDROM drive. The installation program should start automatically.
2. ___ At the Installation Welcome window, select **Install**.
3. ___ Select the **DB2 Enterprise Edition** and **DB2 Application Development Client components**, (see Figure 2–1). Select **Next** to continue.



Select the product(s) you would like to install.

☑ DB2 Enterprise Edition
☑ DB2 Application Development Client
☐ DB2 Administration Client

Description

DB2 Universal Database Enterprise Edition lets you create and manage databases as well as allowing remote client applications to access data on host databases.

Figure 2–1 *DB2 Select Products Window*

Remember, the Library Server and the Content Manager System Administration Client require the DB2 Application Development Client. The Library Server uses the APIs found in the DB2 Application Development Client to dynamically generate access modules (DLLs). These access modules allow static queries to be performed (as opposed to dynamic queries), which reduces the amount of time needed to perform a search. If you forget to install the DB2 Application Development Client on the Library Server, then the item-type access modules (including the initial system defined ones) will not be generated. As a result, you will not be able to create item-types, import documents, and logon to the system!

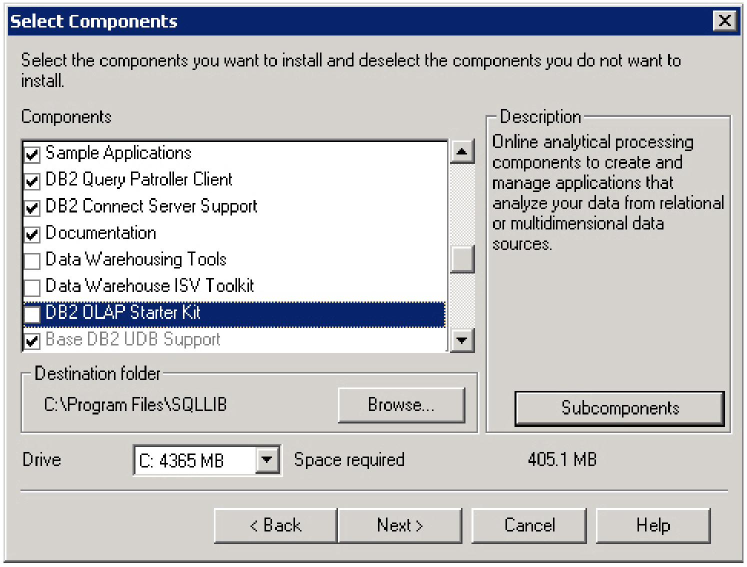
Note: The Content Manager System Administration Client requires the DB2 Application Development Client.

The Content Manager System Administration Client uses the JDBC driver found in the DB2 Application Development Client to access the Library

Server. Therefore, if you were to install the System Administration Client on a separate machine from the Library Server, you must first run the DB2 UDB Installation Program, and choose to install the DB2 Application Development Client component. (Do not forget to apply the DB2 special Fixpack 7 as well!) If this DB2 component does not get installed, one of the first error messages which you will see is "*SQL1109N The specified DLL 'ICMNLSSP' could not be loaded*".

4. ___ Choose the **custom** installation type, and select **Next** to continue.

5. ___ Unselect **only** the *Data Warehousing Tools*, *Data Warehousing ISV Toolkit*, and *DB2 OLAP Starter Kit* components. Leave the other components at their default setting, (see Figure 2–2).



Select Components

Select the components you want to install and deselect the components you do not want to install.

Components

☑ Sample Applications
☑ DB2 Query Patroller Client
☑ DB2 Connect Server Support
☑ Documentation
☐ Data Warehousing Tools
☐ Data Warehouse ISV Toolkit
☐ DB2 OLAP Starter Kit
☑ Base DB2 UDB Support

Description
Online analytical processing components to create and manage applications that analyze your data from relational or multidimensional data sources.

Destination folder
C:\Program Files\SQLLIB

Drive: C: 4365 MB
Space required: 405.1 MB

Figure 2–2 *DB2 Select Components Window*

Although a typical installation could have been performed, unnecessary components (of significant size) would have been installed. (For example, Data Warehousing.) Although these components do not affect Content Manager, reducing the amount of components to be installed can save installation time.

6. ___ Select **Next** to continue.

7. ___ Choose to create the default DB2 instance and select **Next** to continue.

8. ___ Select **Next** to accept the default DB2 Services configuration and continue.

9. ___ Specify **db2admin** as both the *username* and *password* for the Control Center server. Leave the checkbox labeled **Use the same values for the remaining DB2 username and password settings** checked. Select **Next** to continue.

If prompted, choose **Yes** to allow the setup program to create the username. Allowing the setup program to create the username is preferable to manually creating it, as the setup program will ensure that the necessary rights (including advanced rights) are granted.

10. ___ Select **Next** to start copying the files.

11. ___ Select **Finish** to complete the DB2 setup.

12. ___ At the *First Steps* window, select **Exit**. (There is no need to perform any of the First Steps options in this exercise.)

DB2 Text Information Extender (TIE)

IBM$^{(R)}$ DB2$^{(R)}$ UDB Text Information Extender *v7.2 with Fixpack 1 or higher* is required if you plan to use the *Text Search* feature of Content Manager. By using DB2 TIE, clients can perform text searches on attributes and/or document contents. (In previous versions of Content Manager, clients were only able to perform text searches on document contents.) Clients can now perform text searches within sections of structured documents with version 8.1. For example, a user may want to limit a search to a specific tag within an XML document.

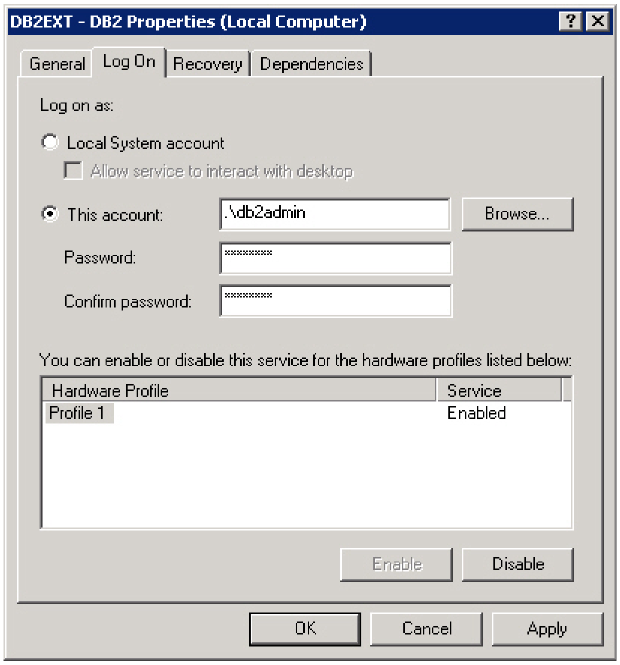
If you do not require text search capabilities, then you do not need to install DB2 TIE. However, if you suspect that this functionality will be needed in the future, it is best to install DB2 TIE before installing Content Manager (as the Content Manager installation program will automatically enable the Library Server database to search for text).

The chapter, *Installing Prerequisites*, in the publication entitled *Planning and Installing Your Content Management System* (GC27-1332), provides detailed instructions for installing DB2 TIE on the various operating system platforms.

Note: Text Information Extender (TIE) must be installed on the same workstation as the Library Server.

The following exercise provides instructions for installing the DB2 Text Information Extender on your Windows workstation.

1. ___ Start the DB2 TIE installation by running `setup.exe`.
2. ___ Choose **English** as the setup language and select **OK** to continue.
3. ___ At the Welcome screen, select **Next** to continue.
4. ___ Select **Next** to accept the destination directory. The DB2 TIE files will be copied.
5. ___ Go to the *Windows Services* control panel and find the service named **DB2EXT - DB2**. This is the DB2 Text Information Extender server. Modify this service so that the start-up type is **Automatic** AND have it logon using the **db2admin** username (see Figure 2–3).



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: .\db2admin

Password: ********

Confirm password: ********

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

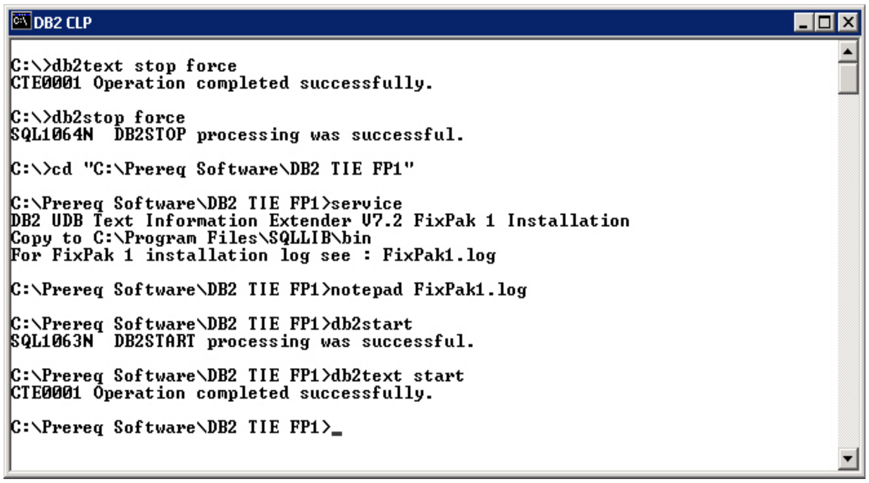
Figure 2–3 *Updating the DB2 TIE Service Log on Name*

Note: It is very important that this service logon with a valid username and **not** as a **Local System Account**. The Content Manager text search feature will be unstable, or may not work at all, if the text search service uses the Local System Account.

6. ___ Start the DB2 TIE service (**DB2EXT - DB2**). You should not receive any error messages.

At this point, you have successfully installed DB2 TIE V7.2, and are now ready to install **Fixpak 1**.

7. ___ Go to a DB2 command window by selecting **Start | Programs | IBM DB2 | Command Window** (see Figure 2–4).



```
C:\>db2text stop force
CTE0001 Operation completed successfully.

C:\>db2stop force
SQL1064N  DB2STOP processing was successful.

C:\>cd "C:\Prereq Software\DB2 TIE FP1"

C:\Prereq Software\DB2 TIE FP1>service
DB2 UDB Text Information Extender V7.2 FixPak 1 Installation
Copy to C:\Program Files\SQLLIB\bin
For FixPak 1 installation log see : FixPak1.log

C:\Prereq Software\DB2 TIE FP1>notepad FixPak1.log

C:\Prereq Software\DB2 TIE FP1>db2start
SQL1063N  DB2START processing was successful.

C:\Prereq Software\DB2 TIE FP1>db2text start
CTE0001 Operation completed successfully.

C:\Prereq Software\DB2 TIE FP1>_
```

Figure 2–4 *Installing DB2 TIE Fixpak 1*

8. ___ Before installing this Fixpak, the TIE instance and database manager must be stopped. From within this DB2 command window, type `db2text stop force` and press **Enter**. Then type `db2stop force` and press **Enter** (see Figure 2–4).

9. ___ Change to the directory containing Fixpack 1. Install the DB2 TIE Fixpak 1 by typing `service` and pressing **Enter**. You should see a message similar to what is shown in Figure 2–4. You may also want to type `notepad FixPak1.log` to check for any errors which may have occurred during the Fixpak installation.

10. ___ Start the database manager by typing `db2start`. Start the text search server by typing `db2text start`.

Install DB2 v7.2 Special Fixpak 7 for CM

When used with Content Manager for Multiplatforms, DB2 UDB requires a special build of DB2 Fixpack 7. The special build includes some fixes which allow Content Manager to operate properly. DB2 Special Fixpack 7 for Content Manager can be downloaded from the following location:

http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/fp7_cm.d2w/report

The DB2 UDB fixpak should always be installed **after** DB2 TIE and any DB2 TIE Fixpak. In other words, if you apply a DB2 UDB fixpak, and then install DB2 TIE (and/or DB2 TIE fixpak), you should reapply the DB2 UDB fixpak. This will ensure that the DB2 UDB files are at proper levels.

1. ___ Start the DB2 UDB v7.2 Fixpak installation by running `setup.exe`.
2. ___ Select **Next** to accept the destination directory.
3. ___ Select **Next** to start copying the files.
4. ___ Select **Finish** to complete the Fixpak installation.

> **Note:** After applying DB2 UDB Fixpaks, you must always rebind your databases. The procedure for doing so is described in the Fixpak Readme file under the section entitled *Rebinding to Non-DRDA DB2 Databases*. Because this exercise is a new installation, you have no user databases that must be rebound.

For additional information related to DB2 TIE, refer to the *DB2 Text Information Extender Administration and User's Guide*. You can find this document on the DB2 Universal Database Text Information Extender CDs included with the Content Manager package.

IBM WebSphere Application Server

IBM WebSphere Application Server (WAS) v4.0 *(with PTF 3 or higher)* is required for the Resource Manager. The Resource Manager replaces what previous versions of Content Manager referred to as the Object Server, and is used to manage documents within the Content Management system. The Resource Manager is deployed as a J2EE web application, and thereby requires a J2EE compliant application server. Although any application server should work with the Resource Manager, only the WebSphere Application Server is officially supported.

The Content Manager V8 packaging includes WebSphere Application Server Advanced Single Server Edition (AEs). However, WebSphere Application Server Advanced Edition (AE) is also supported, and would allow the Resource Manager to leverage such capabilities as clustering and cloning.

The chapter, *Installing Prerequisites*, in the publication entitled *Planning and Installing Your Content Management System* (GC27-1332), provides detailed instructions for installing WebSphere Application Server AEs on the various operating system platforms.

> **Note:** WAS must be installed and configured before you begin the installation of the Content Manager Resource Manager component, and it must be installed on the same workstation as the Resource Manager.

The following exercise provides instructions for installing WebSphere Application Server AEs on your Windows workstation.

1. ___ WebSphere requires that the DB2 JDBC be v2.0. Update the DB2 JDBC from v1.0 to v2.0 by going to `C:\Program Files\SQLLIB\java12` and run `usejdbc2.bat`.
2. ___ Start the WebSphere Application Server (WAS) installation by running `setup.exe`.
3. ___ Choose **English** as the setup language and select **OK** to continue.
4. ___ At the Welcome screen, select **Next** to continue.
5. ___ Choose the **custom** installation type, and select **Next** to continue.
6. ___ Leave all components checked, and select **Next** to continue.

> **Note:** : Although WebSphere could be used with Microsoft Internet Information server, you will be installing the IBM HTTP Server. In order to avoid a conflict between the two HTTP servers, you should either make sure both servers are not using port 80, or disable Microsoft Internet Information server entirely by disabling the Windows service named "World Wide Web Publishing."

7. ___ At the *Choose Webserver Plug-ins* window, make sure the **IBM HTTP Server** is checked and select **Next** to continue.
8. ___ Specify **admin** as the *username* (with a *password* of **password**) to be used to start the IBM HTTP Server.

9. ___ Accept the default destination directories and select **Next** to continue.

10. ___ Accept the default program folder and select **Next** to continue.

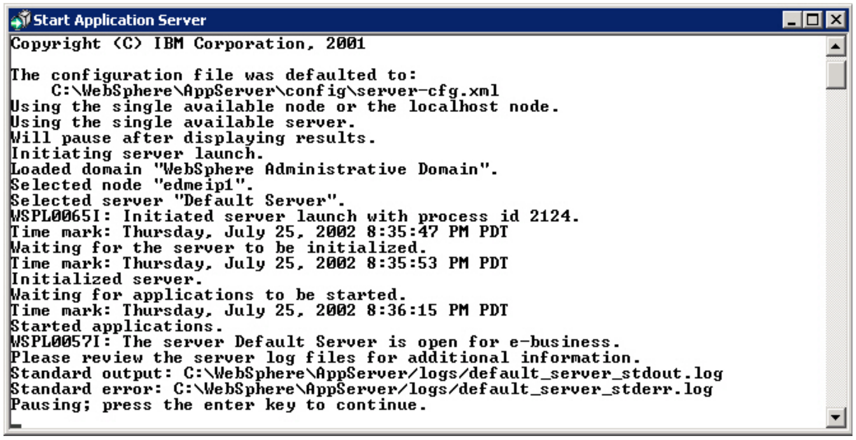
11. ___ Select **Next** to confirm your choices and to start copying the files.

12. ___ Select **Finish** to complete the setup and choose to **restart** the computer now.

13. ___ **Close** the *First Steps Wizard* (which appears after the computer restarts and you login).

Before installing any WebSphere PTFs, it is a good idea to test the installation of WebSphere. This not only ensures a successful installation of WebSphere, but also ensures that the HTTP server plug-in was configured properly.

14. ___ Start the WebSphere Application Server by going to **Start** | **Programs**, **IBM WebSphere** | **Application Server V4.0 AEs** | **Start Application Server**. You should see a message saying, "*The server Default Server is open for e-business,*" (see Figure 2–5). Press any key to close the command window (the application server will run in the background).



```
Copyright (C) IBM Corporation, 2001

The configuration file was defaulted to:
    C:\WebSphere\AppServer\config\server-cfg.xml
Using the single available node or the localhost node.
Using the single available server.
Will pause after displaying results.
Initiating server launch.
Loaded domain "WebSphere Administrative Domain".
Selected node "edmeip1".
Selected server "Default Server".
WSPL0065I: Initiated server launch with process id 2124.
Time mark: Thursday, July 25, 2002 8:35:47 PM PDT
Waiting for the server to be initialized.
Time mark: Thursday, July 25, 2002 8:35:53 PM PDT
Initialized server.
Waiting for applications to be started.
Time mark: Thursday, July 25, 2002 8:36:15 PM PDT
Started applications.
WSPL0057I: The server Default Server is open for e-business.
Please review the server log files for additional information.
Standard output: C:\WebSphere\AppServer/logs/default_server_stdout.log
Standard error: C:\WebSphere\AppServer/logs/default_server_stderr.log
Pausing; press the enter key to continue.
```

Figure 2–5 *WebSphere Application Server AEs Starting*

15. ___ Open a web browser and go to *http://<hostname>*, where *<hostname>* is the hostname of your machine. You should see the IBM HTTP Server Welcome Page. This means the IBM HTTP Server is active.

If you do not see the IBM HTTP Server Welcome page, try the following:

a. Go to the *Windows Services Control Panel* and be sure the service named **IBM HTTP Server** is running.

b. If the service refuses to start, check for syntax errors in the `httpd.conf` file.

c. Make sure the Microsoft Internet Information HTTP Server is **not** running, by going to the *Windows Services Control Panel* and check that the service named World Wide Web Publishing Service is **not** running.

d. Check the IBM HTTP Server log files in `C:\IBM HTTP Server\logs`.

16. ___ Open a web browser and go to `http://<hostname>/servlet/snoop`, where <*hostname*> is the hostname of your machine. You should see a page entitled **Snoop Servlet - Request/Client Information**. This means that the application server is running and is integrated with the HTTP server.

If you do not see the Snoop Servlet Information page, try the following:

a. Go to the WebSphere Administrator's Console (**Start** | **Programs** | **IBM WebSphere** | **Application Server V4.0 AEs** | **Administrator's Console**), and make sure the `sampleApp` Enterprise Application is running.

b. Make a request directly to WebSphere by going to: `http://<hostname>:9080/servlet/snoop`. If this works, then the web server plug-in needs to either be regenerated or reinstalled. You can regenerate the web server plug-in via the WebSphere Administrator's Console.

c. Check the WebSphere log files in `C:\WebSphere\AppServer\logs`.

Once you have validated that the WebSphere Application Server is working properly, PTF 3 can be applied. If WebSphere is not working, you must correct the problem before applying any PTFs to avoid compounding the problem.

> **Caution:** Applying a WebSphere PTF should be done with much care. Pay close attention to the messages generated by the install program. If you see any errors, they **must** be corrected. (Usually, if you get an error during the PTF install, you must uninstall the PTF, fix the problem, and then reinstall the PTF.) If a PTF does not go on cleanly, then WebSphere will get into an unstable state, and this will affect how Content Manager operates.

17. ___ Before applying any WebSphere PTFs, **both** the WebSphere Application Server **and** HTTP Server **must** be stopped.

Stop the WebSphere Application Server by going to:

`C:\WebSphere\AppServer\bin`

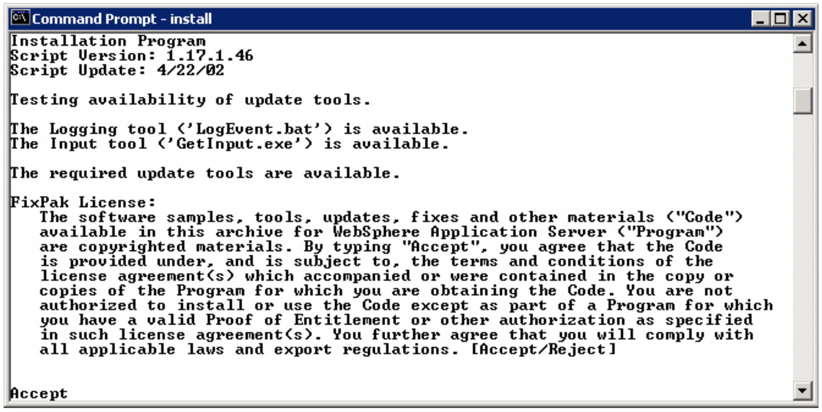
and run `stopServer.bat`.

Stop the IBM HTTP Server by going to the *Windows Services Control Panel*, and stop the services named **IBM HTTP Administration** AND **IBM HTTP Server**.

If you have not done so already, close the WebSphere First Steps Wizard, as it puts locks on files which need to be updated by the PTF.

18. ___ Go to the command prompt (**Start** | **Programs** | **Accessories**, **Command Prompt**).

19. ___ Change to the directory containing PTF 3. Install the WebSphere PTF 3 by typing `install` and pressing **Enter**. You should see a message similar to what is shown in Figure 2–6.



```
Installation Program
Script Version: 1.17.1.46
Script Update: 4/22/02

Testing availability of update tools.

The Logging tool ('LogEvent.bat') is available.
The Input tool ('GetInput.exe') is available.

The required update tools are available.

FixPak License:
   The software samples, tools, updates, fixes and other materials ("Code")
   available in this archive for WebSphere Application Server ("Program")
   are copyrighted materials. By typing "Accept", you agree that the Code
   is provided under, and is subject to, the terms and conditions of the
   license agreement(s) which accompanied or were contained in the copy or
   copies of the Program for which you are obtaining the Code. You are not
   authorized to install or use the Code except as part of a Program for which
   you have a valid Proof of Entitlement or other authorization as specified
   in such license agreement(s). You further agree that you will comply with
   all applicable laws and export regulations. [Accept/Reject]


Accept
```

Figure 2–6 *Installing the WebSphere Application Server PTF*

20. ___ Follow the prompts and the following points to guide you through the PTF installation:

- **a.** Update the Application Server
- **b.** The Application Server Home is `C:\WebSphere\AppServer`
- **c.** Use the Application Server JDK
- **d.** Update the JDK
- **e.** **Do not** update the iPlanet web server (You do not have iPlanet

installed.)

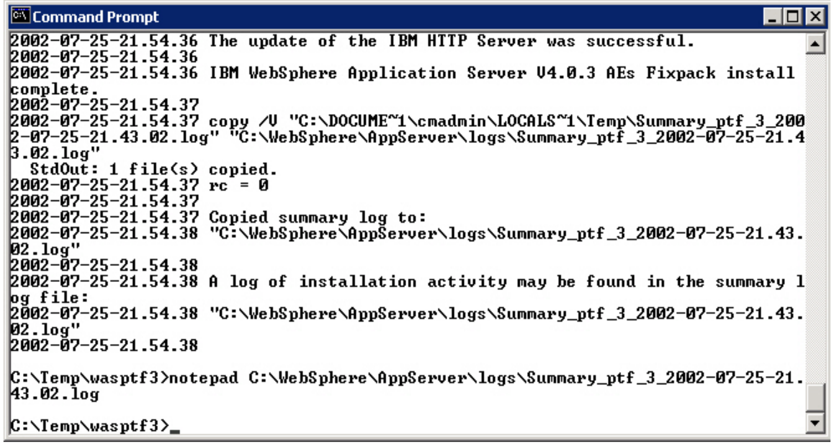
f. Update the IBM HTTP Server

g. The IBM HTTP Server home is `C:\IBM HTTP Server`

h. Use the Application Server's log directory

i. Place the backups under the WebSphere Application Server Home

21. ___ When the PTF installation is complete, a message will indicate where the installation activity log file may be found (see Figure 2–7). Open this log file in notepad, and scan for any errors. If you do see an error, you **must** uninstall the PTF (by running `C:\WebSphere\AppServer\uninstall_ptf_3.bat`), correct the problem, and then reinstall the PTF.



```
2002-07-25-21.54.36 The update of the IBM HTTP Server was successful.
2002-07-25-21.54.36
2002-07-25-21.54.36 IBM WebSphere Application Server V4.0.3 AEs Fixpack install
complete.
2002-07-25-21.54.37
2002-07-25-21.54.37 copy /V "C:\DOCUME~1\cmadmin\LOCALS~1\Temp\Summary_ptf_3_200
2-07-25-21.43.02.log" "C:\WebSphere\AppServer\logs\Summary_ptf_3_2002-07-25-21.4
3.02.log"
  StdOut: 1 file(s) copied.
2002-07-25-21.54.37 rc = 0
2002-07-25-21.54.37
2002-07-25-21.54.37 Copied summary log to:
2002-07-25-21.54.38 "C:\WebSphere\AppServer\logs\Summary_ptf_3_2002-07-25-21.43.
02.log"
2002-07-25-21.54.38
2002-07-25-21.54.38 A log of installation activity may be found in the summary l
og file:
2002-07-25-21.54.38 "C:\WebSphere\AppServer\logs\Summary_ptf_3_2002-07-25-21.43.
02.log"
2002-07-25-21.54.38

C:\Temp\wasptf3>notepad C:\WebSphere\AppServer\logs\Summary_ptf_3_2002-07-25-21.
43.02.log

C:\Temp\wasptf3>_
```

Figure 2–7 *Checking the PTF Install Log After Installation*

22. ___ Start the IBM HTTP Server by going to the *Windows Services Control Panel* and starting the services named **IBM HTTP Administration** and **IBM HTTP Server**.

23. ___ Repeat Steps 14-16 to start the WebSphere Application Server and verify that the PTF was installed properly.

Microsoft Visual C++

On Windows, the Content Manager Library Server requires the Microsoft Visual C++ v6.0 compiler in order to dynamically build access modules (DLLs). These access modules are built when item types are created and when static queries (as opposed to slower dynamic queries) need to be created. The compiler must be installed, and environment variables need to be properly configured in order for the Content Manager installation program to be successful. (As part of the install, the Content Manager installation program will create system defined libraries.)

1. ___ Insert the Microsoft Visual C++ v6.0 CD into your CDROM drive. The installation program should start automatically.

2. ___ Choose to perform a **typical installation**.

Note: When prompted to by the installation program, you **must** choose to register environment variables.

3. ___ Choose **register environment variables** (prompted after the file copy process). This will cause the installation program to update the *INCLUDE*, *LIB*, and *PATH* environment variables with the necessary Microsoft Visual C++ directories.

Note: You must change user variables to system variables, making sure that you place the DB2 values **before** the Visual C++ values.

Configure Environment Variables

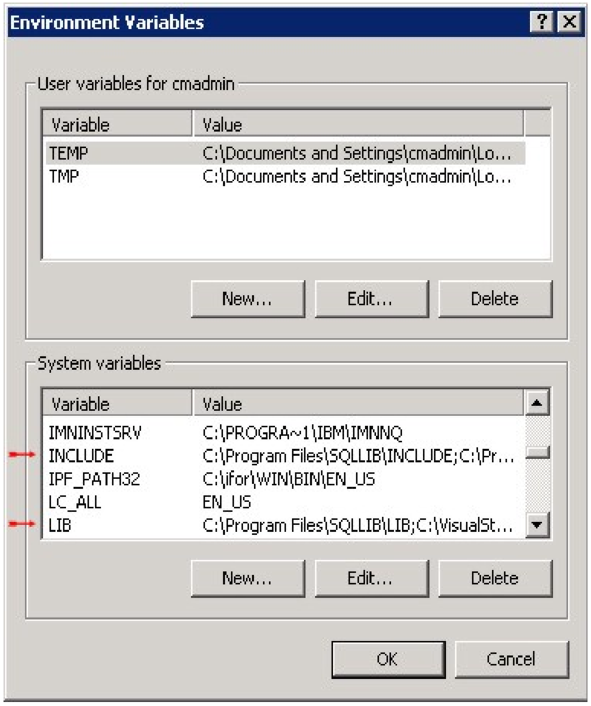
As stated earlier, the Library Server uses the Microsoft Visual C++ compiler and the DB2 Application Development Client to dynamically build *access modules* (DLLs) for item-types (previously known in Content Manager version 7 as index classes). In order for the build to be successful, the DB2 UDB directories must be listed **before** the Microsoft Visual C++ directories in the *INCLUDE*, *LIB*, and *PATH* environment variables.

Note: Both products contain a common header (`*.h`) file. If the Microsoft Visual C++ directories are listed first, then its header file will be used and the build will fail. (This problem is specific to the Windows platform.)

1. ___ Go to the Windows Control Panel and open System. On the tab labeled *Advanced*, select the **Environment Variables** button.

2. ___ Move the Microsoft Visual C++ USER variables to the **SYSTEM** variables section. In doing so, you will need to **APPEND** the user *INCLUDE*,

LIB, and *PATH* variables to the system *INCLUDE*, *LIB*, and *PATH* variables respectively. Remember to make sure the DB2 UDB directories are listed **before** the Microsoft Visual C++ directories (see Figure 2–8).



User variables for cmadmin

Variable	Value
TEMP	C:\Documents and Settings\cmadmin\Lo...
TMP	C:\Documents and Settings\cmadmin\Lo...

System variables

Variable	Value
IMNINSTSRV	C:\PROGRA~1\IBM\IMNNQ
INCLUDE	C:\Program Files\SQLLIB\INCLUDE;C:\Pr...
IPF_PATH32	C:\ifor\WIN\BIN\EN_US
LC_ALL	EN_US
LIB	C:\Program Files\SQLLIB\LIB;C:\VisualSt...

Figure 2–8 *Environment Variables Configured Properly*

3. ___ Select **OK** to save your changes. Verify the environment variable changes by going to a command window (**Start | Programs**, **Accessories | Command Prompt**) and typing the following:
   a. `set include`
   b. `set lib`
   c. `set path`

You should see the values of each environment variable. Make sure the DB2 UDB directories are listed **before** the Microsoft Visual C++ directories. The following is an EXAMPLE of what your variables should include:

```
INCLUDE=C:\Program Files\SQLLIB\INCLUDE;
C:\Program Files\SQLLIB\LIB;
C:\Program Files\Microsoft Visual Studio\VC98\atl\include;
C:\Program Files\Microsoft VisualStudio\VC98\mfc\include;
C:\Program Files\Microsoft Visual Studio\VC98\include
LIB=C:\Program Files\SQLLIB\LIB;
C:\Program Files\Microsoft Visual Studio\VC98\mfc\lib;
C:\Program Files\Microsoft Visual Studio\VC98\lib
Path=C:\WINDOWS\system32;
C:\WINDOWS;C:\WINDOWS\System32\Wbem;
C:\Program Files\SQLLIB\BIN;
C:\Program Files\SQLLIB\FUNCTION;
C:\Program Files\SQLLIB\SAMPLES\REPL;
C:\Program Files\SQLLIB\HELP;
C:\Program Files\Microsoft Visual Studio\Common\Tools\WinNT;
C:\Program Files\Microsoft Visual Studio\Common\MSDev98\Bin;
C:\Program Files\Microsoft Visual Studio\Common\Tools;
C:\Program Files\Microsoft Visual Studio\VC98\bin
```

At this point, the prerequisite software needed to continue the exercises in the next chapter have been installed. All the necessary Fixpaks have also been applied. You are now ready to begin the Content Manager Version 8.1 installation in the following chapter.

Tivoli Storage Manager

The Tivoli Storage Manager (TSM) is an optional feature that provides *long-term storage* on devices other than the fixed disks attached to the Resource Manager. If you intend to store your documents only on fixed disks, then TSM is not needed. However, by using TSM, you can leverage such features as offsite storage and comprehensive backup of your data for disaster recovery. TSM can be installed after the Resource Manager component is installed.

Instructions for installing and configuring the TSM are provided in the section entitled *Installing and Configuring the Tivoli Storage Manager* in the *Planning and Installing Your Content Management System* (GC27-1332) publication.

More detail on the Tivoli Storage Manager, as well as an installation and configuration exercise, can be found later in Chapter 12 of this study guide.

LDAP Server

Content Manager Version 8.1 supports a variety of Lightweight Directory Access Protocol (LDAP) Servers. At the time of this writing, the following LDAP servers have been tested with Content Manager Version 8.1:

- IBM Directory Server (previously named IBM(R) Directory Server Version 4.1)
- Microsoft Active Directory
- Lotus Domino Directory Notes Address Book (NAB)

An LDAP server provides a central repository for information, such as server definitions and user accounts. Instead of having to create user IDs on every server in the enterprise, an administrator may choose to store this information in an LDAP server.

By integrating Content Manager with an LDAP server, an administrator can use the Content Manager System Administration client to import existing user definitions. User names must be imported into the Content Manager system so that the Content Manager access control can be configured. However, passwords are not imported. Instead, when attempting to logon to a Library Server, a user will be authenticated by the LDAP server. By implementing an LDAP server, users only need to maintain their password in one location. The benefit of an LDAP server grows as more servers in your enterprise use LDAP for authentication.

An LDAP server can be integrated either during or after the Content Manager installation. Instructions for configuring the LDAP integration are provided in the section entitled *Enabling LDAP* in the *Planning and Installing Your Content Management System* (GC27-1332) publication.

More detail on LDAP integration with Content Manager, as well as an installation and configuration exercise, can be found in Chapter 8 of this study guide.

Installing Prerequisites on AIX and Solaris

The prerequisite software required for Content Manager on AIX and Solaris is similar to what is required on the Windows platform. In order to install the Content Manager server on the UNIX platform, you should install the following:

- IBM DB2 Universal Database
- DB2 Text Information Extender (TIE)
- IBM WebSphere Application Server (AE or AEs)
- VisualAge C++ Professional Batch Compiler *(for AIX operating systems)*
- Forte C++ Compiler Enterprise Edition *(for Solaris operating systems)*
- Tivoli Storage Manager (only required for storage other than DASD)

The software packages listed above provide the same functions as they do on the Windows platform. Notice that a C++ compiler is still required (although each platform uses a different one).

Be particularly careful when installing the C++ compiler on UNIX. Unlike the Windows platform, you must properly license the compiler to the Library Server user ID. The best way to test the compiler installation is to use the Library Server user ID (for example, *icmadmin*) to compile and run a sample C++ program.

Instructions for installing and configuring these prerequisite software on UNIX can be found in the publication entitled *Planning and Installing Your Content Management System* (GC27-1332) and the *Content Manager QuickStart Guide*.

Summary

In this chapter, you reviewed the prerequisite software that is required to install a Content Management system. Detailed instructions for installing this software on the Windows platform were also provided.

DB2 UDB is required by both the Library Server and Resource Manager to store information such as user accounts, access privileges, document information, and storage management configurations.

The DB2 Application Development Client is required by the Library Server so that dynamically generated libraries could be built. It is also required by the Content Manager System Administration client for communication with the Library Server.

IBM(R) DB2(R) UDB Text Information Extender is required to provide text search capabilities for your Content Management system. It allows clients to perform text searches on both metadata and/or document contents. DB2 TIE must be installed on the Library Server workstation.

WebSphere Application Server (WAS) is required by the Resource Manager. The Resource Manager is a web application, and requires an application server to host it. Both Advanced Edition Single Server (AEs) or Advanced Edition (AE) are supported by the Resource Manager. Furthermore, the capabilities provided by WAS, such as clustering and cloning, can be leveraged by the Resource Manager.

A compiler is also required by the Library Server so that static queries can be dynamically generated. Shared libraries are also built when item types are created. If the compiler is not installed and configured properly, then item type creation will fail. The creation of static queries allows for the increased query performance, and can dynamically change based on what clients are searching for.

Tivoli Storage Manager (TSM) is optional, and is only required by the Resource Manager if you want to store objects on a device other than hard disk. For example, if you would like to store rarely accessed documents in an optical jukebox, then you must install TSM.

An LDAP server is also optional, and is only required if you want to provide a central repository to store user and server information. By using an LDAP server, users only need to maintain their passwords in one place.

CHAPTER 3

Installing Content Manager

- User IDs and Connections
- Library Server
- Resource Manager
- Client for Windows
- Content Manager First Steps
- Important Files

In this chapter, you will learn how to install IBM Content Manager Version 8.1 on the Windows platform. User ID management, database connections, and secured sockets layer will be discussed. Lastly, important files created by the install program will be described.

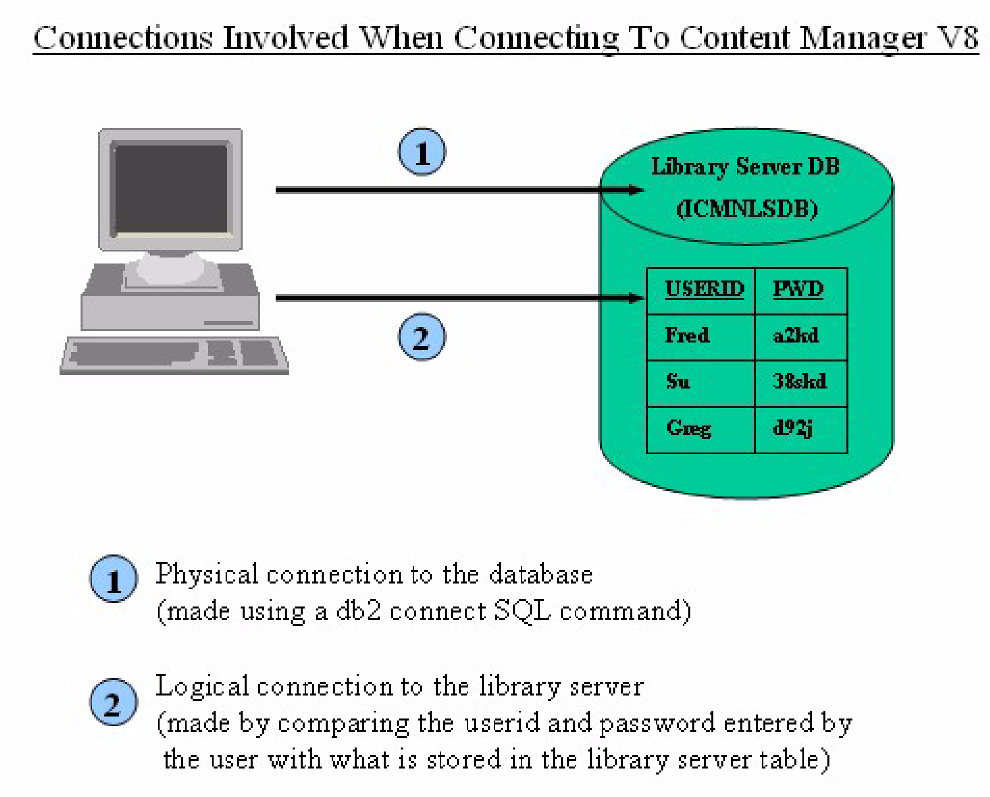
Before beginning the exercises contained within this chapter, all prerequisite software should already be installed and configured (see Chapter 2, *Installing Prerequisites*).

User IDs and Connections

Before installing Content Manager Version 8.1, it is **important** to understand the distinction between system user IDs and Content Manager user IDs. A *system user ID* is one that is created with the operating system tools (for example, Microsoft Windows or AIX), and is the user ID you normally use to log into the machine. A *Content Manager user ID* is created in the Content Manager System Administration client, and is the user ID you use to login to the Content Manager Library Server. Understanding the distinction between the two different types of user IDs is key to understanding the underlying communication channel between the Content Manager servers and clients.

Connection Types

In order to login to the Content Manager Library Server, the connecting user must have a means of connecting to the Library Server database *ICMNLSDB*. The login request must be able to validate the specified Content Manager user ID and password with what is stored in the Library Server database tables. If a connection to the database cannot be made, then there is no way to check the Content Manager user ID and password. This will result in a login failure. The Library Server database must be registered on client machines so that the database connection can be made. Figure 3–1 depicts the two types of connections involved when connecting to a Content Manager Library Server.



Connections Involved When Connecting To Content Manager V8

USERID	PWD
Fred	a2kd
Su	38skd
Greg	d92j

1 Physical connection to the database
(made using a db2 connect SQL command)

2 Logical connection to the library server
(made by comparing the userid and password entered by the user with what is stored in the library server table)

Figure 3–1 *Connection Types*

Connection Process

The username used to make the physical database connection will either be the Content Manager username entered by the client, or will be a shared database connection ID. When a client signs onto Content Manager, he/she enters a username and password. The APIs will try to connect to the Library Server database using this same username and password. This is done by executing `db2 connect to <db name> user <username> using <password>`. If the connection fails, the APIs will try to use a shared database connection user ID. Once the database connection is made, the APIs will query the Library Server user table so that the supplied username and password can be checked. The flowchart in Figure 3–2 depicts how the Content Manager connection logic is handled:

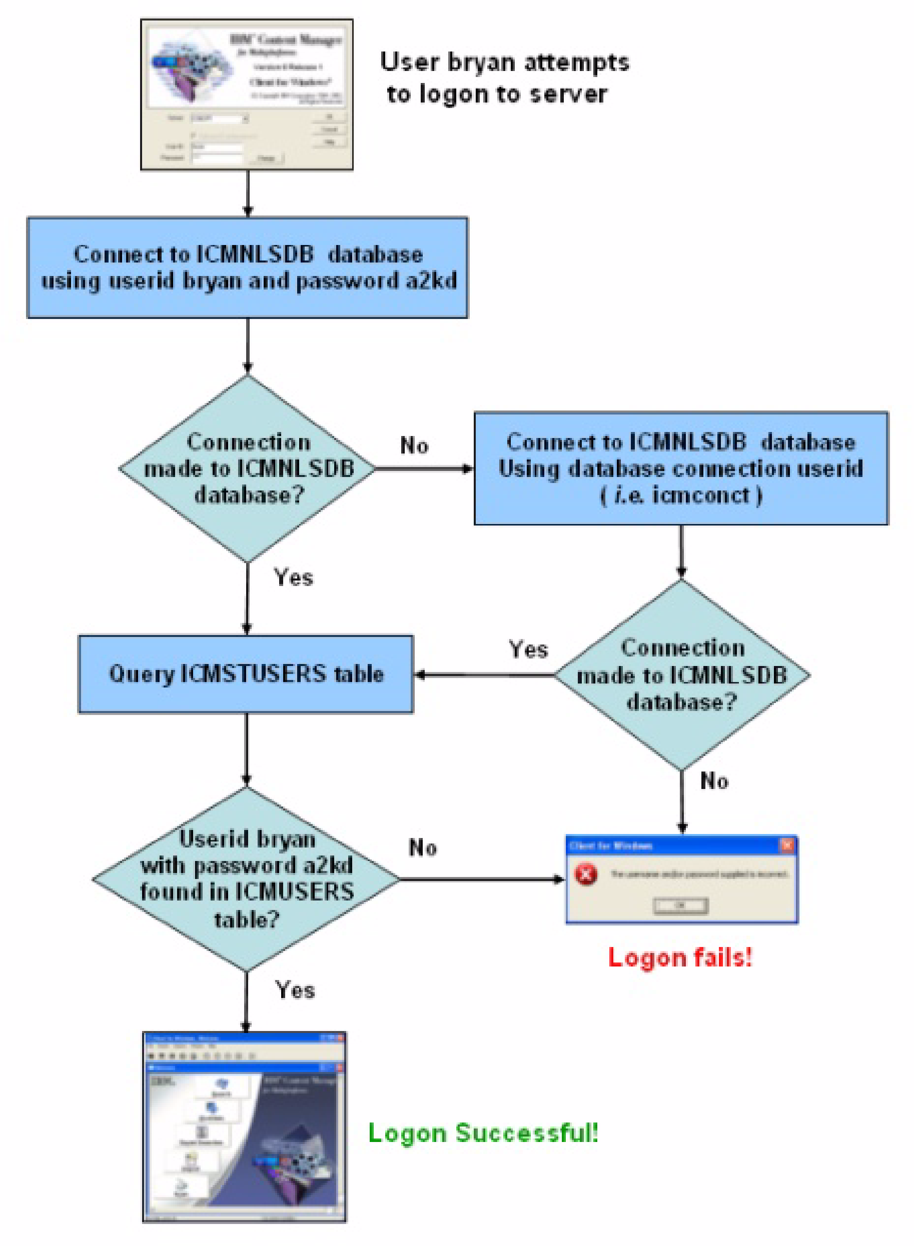

User bryan attempts to logon to server
Connect to ICMNLSDB database using userid bryan and password a2kd
Connection made to ICMNLSDB database?
No
Connect to ICMNLSDB database Using database connection userid (i.e. icmconct)
Yes
Query ICMSTUSERS table
Yes
Connection made to ICMNLSDB database?
No
Userid bryan with password a2kd found in ICMUSERS table?
No
Logon fails!
Yes
Logon Successful!

Figure 3–2 *Content Manager Connection Logic*

Database Connections

One **important** concept you must grasp is how database connection request are authenticated by DB2 UDB. The most common form of database authentication occurs at the local operating system. (DB2 can be configured so that authentication can be performed against a Windows Domain or LDAP Server.) When a user ID and password are supplied for a database connection request (for example, `db2 connect to icmnlsdb user su using 38skd`), DB2 will pass the user ID and password to the operating system for example, Microsoft Windows) for authentication. If a system user ID with the same password already exists, then the database connection is allowed. However, if the system user ID does not exist, or if the password is different, then the authentication will fail and the database connection request will be denied.

When installing Content Manager, you are asked whether server authentication or client authentication should be used. The type of authentication is configured at the database instance, and is set to server by default. When server authentication is used, DB2 will authenticate the user ID and password on the DB2 server operating system. This means that any system user IDs you create for the database connection must be created on the DB2 server. Likewise, when client authentication is used, DB2 will authenticate the user ID and password on the client operating system.

Required System User IDs

The Content Manager installation guide recommends that you create two system user IDs for the Library Server (for example, *icmadmin* and *icmconct*), and one user ID for the Resource Manager (for example, *rmadmin*).

- The *icmadmin* user ID should have administrative authority to the Library Server database because it is used for administrative functions.
- The *icmconct* user ID only needs connect privileges to the Library Server database because regular Content Manager user IDs share this user ID to perform database queries.
- The *rmadmin* user ID should have administrative authority to the Resource Manager database because it will be used by the Resource Manager server to perform administrative functions to the Resource Manager database.

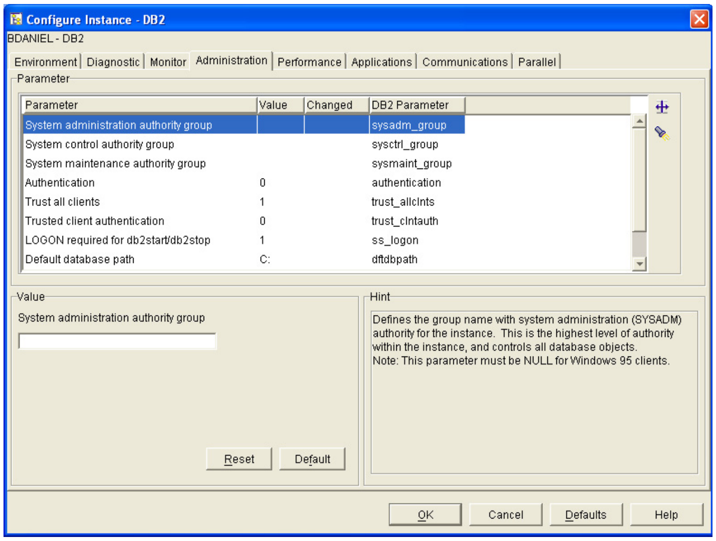
Database Administrative Authority

The db2 parameter named *sysadm_group* specifies the name of the system group which has DB2 administrative authority. Any users which belong to this group will have administrative authority to the databases managed by the DB2 instance.

By default, the *sysadm_group* parameter has no value. This means that any system user ID that is a member of the Administrator's system group will have DB2 system administration authority. If you would like to create a DB2 administration user ID, but do not want this user ID to be an administrator on the local machine, the following steps can be done:

1. ___ Create a unique system group name like *dbadm* (or any name you prefer).
2. ___ Assign any user IDs (for example, *icmadmin* and *rmadmin*) that needs DB2 administrative authority to the *dbadm* group.
3. ___ Update the DB2 *sysadm_group* parameter to *dbadm*.

The DB2 Control Center (**Start | Programs | IBM DB2 | Control Center**) can be used to update this parameter. From the DB2 Control Center, right-click on the instance name (default name is *DB2*), and choose **Configure** from the context menu. The Configure Instance Window (see Figure 3–3) will appear. The *sysadm_group* parameter is found on the page labeled **Administration**.



Parameter	Value	Changed	DB2 Parameter
System administration authority group			sysadm_group
System control authority group			sysctrl_group
System maintenance authority group			sysmaint_group
Authentication	0		authentication
Trust all clients	1		trust_allclnts
Trusted client authentication	0		trust_clntauth
LOGON required for db2start/db2stop	1		ss_logon
Default database path	C:		dftdbpath

System administration authority group

Defines the group name with system administration (SYSADM) authority for the instance. This is the highest level of authority within the instance, and controls all database objects.
Note: This parameter must be NULL for Windows 95 clients.

Figure 3–3 *Configure Instance Window*

Before beginning the Content Manager installation, be sure to complete the following steps:

1. ___ Create a system user ID called *icmadmin*. Set the password to *password*. Grant *icmadmin* DB2 system administration authority by assigning it to the Administrators group. (If you specified a group name for the DB2 *sysadm_group*, then assign *icmadmin* to that group instead.)

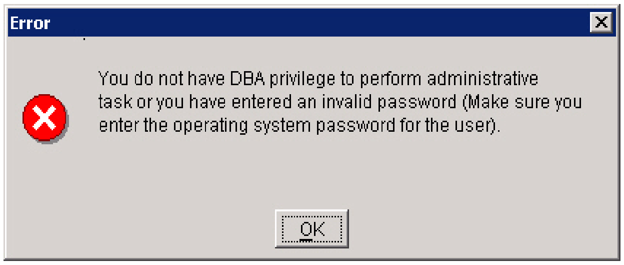
2. ___ Create a system user ID called *rmadmin*. Set the password to *password*. Grant *rmadmin* DB2 system administration authority by assigning it to the Administrators group. (If you specified a group name for the DB2 *sysadm_group*, then assign *rmadmin* to that group instead.)

3. ___ Create a system user ID called *icmconct*. Set the password to *password*. Assign *icmconct* to the Users group. (Do **not** grant administrative authority to this user ID, because regular Content Manager users use and or share this user ID.)

Administrators and Database Authority

After installing Content Manager, if you create any other Content Manager administrator user IDs, you must also create a corresponding system user ID and grant it DB2 system administration authority. The reason you must do this is because Content Manager administrators may need to perform administrative functions to the database when configuring Content Manager (for example, creating item types).

Figure 3–3 shows, when trying to sign on to Content Manager, the APIs will first try to connect to the database using the same user ID and password. If this fails (because there is no system user ID with the same user ID and password), then the APIs will try to use the database connection ID (for example, icmconct). However, because this database connection ID does not have database administration authority, you will see the error message shown in Figure 3–4.



You do not have DBA privilege to perform administrative task or you have entered an invalid password (Make sure you enter the operating system password for the user).

Figure 3–4 *Sign on Error Message*

Installing Content Manager on Windows

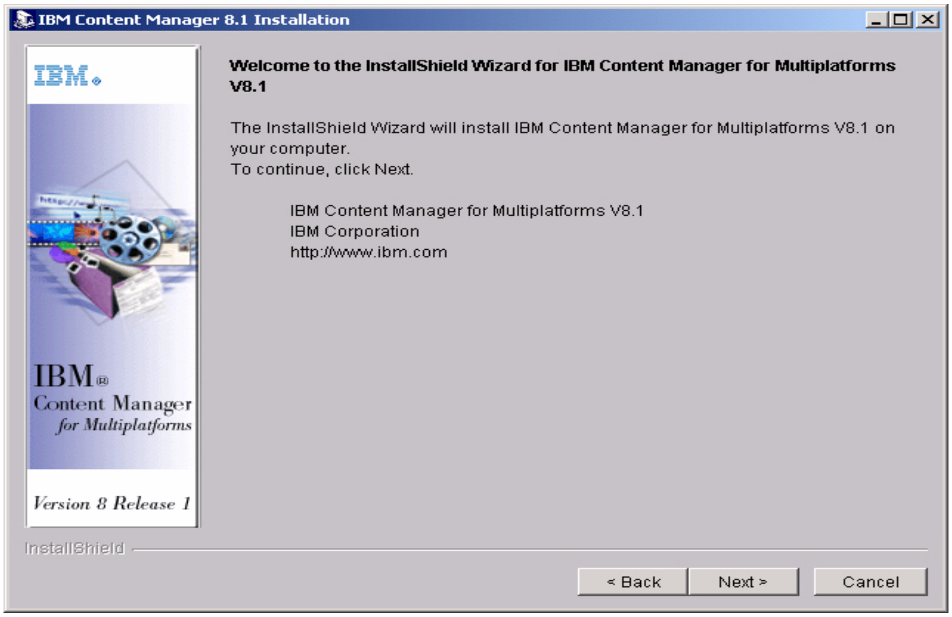
Be certain the following conditions are met before installing Content Manager:

1. ___ Make sure that the person who installs Content Manager is an administrator. (The user ID that is going to install the server must be a member of the Administrators group, has DB2 administrative authority, and is less than or equal to eight characters.)
2. ___ Required system user IDs were created.
3. ___ All prerequisite software is properly installed and configured.

> **Note:** The Content Manager QuickStart Guide (found on the Content Manager documentation CD) is also a great reference for installing a test system on Windows, AIX, and SUN.

Welcome Screen

1. ___ Start the Content Manager installation by inserting the Content Manager CD into the CDROM drive of your workstation. The Content Manager installation launch pad opens and you see the, **Welcome to Content Manager** screen, (see Figure 3–5).



Welcome to the InstallShield Wizard for IBM Content Manager for Multiplatforms V8.1

The InstallShield Wizard will install IBM Content Manager for Multiplatforms V8.1 on your computer.
To continue, click Next.

IBM Content Manager for Multiplatforms V8.1
IBM Corporation
http://www.ibm.com

Figure 3–5 *InstallShield Welcome Screen*

2. ___ At the Installation *Welcome* screen, select **Next** to continue.

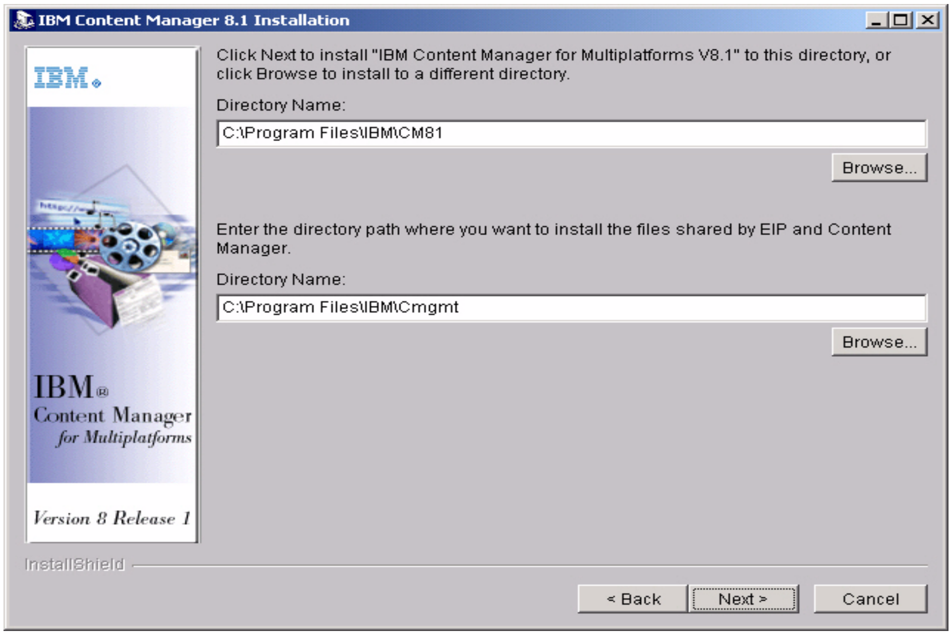
Software License Agreement Panel

Read the Content Manager license terms. If you accept the license terms, select **Accept**. If you do not accept the license terms, the installation program terminates.

3. ___ Select **Next** to continue the installation. The *Select Install Directory* Screen opens.

Install Directory

Figure 3–6 on page 70 shows the *Select Install Directory* screen and offers a choice of where the Content Manager program files will be installed.



Click Next to install "IBM Content Manager for Multiplatforms V8.1" to this directory, or click Browse to install to a different directory.

Directory Name:

C:\Program Files\IBM\CM81

Enter the directory path where you want to install the files shared by EIP and Content Manager.

Directory Name:

C:\Program Files\IBM\Cmgmt

Figure 3–6 *Select Install Directory Screen*

4. ___ Accept the default destination directories, and select **Next** to continue.

Choose Setup

Figure 3–7 shows the Choose Setup screen and offers a choice between a Full or Custom Installation.

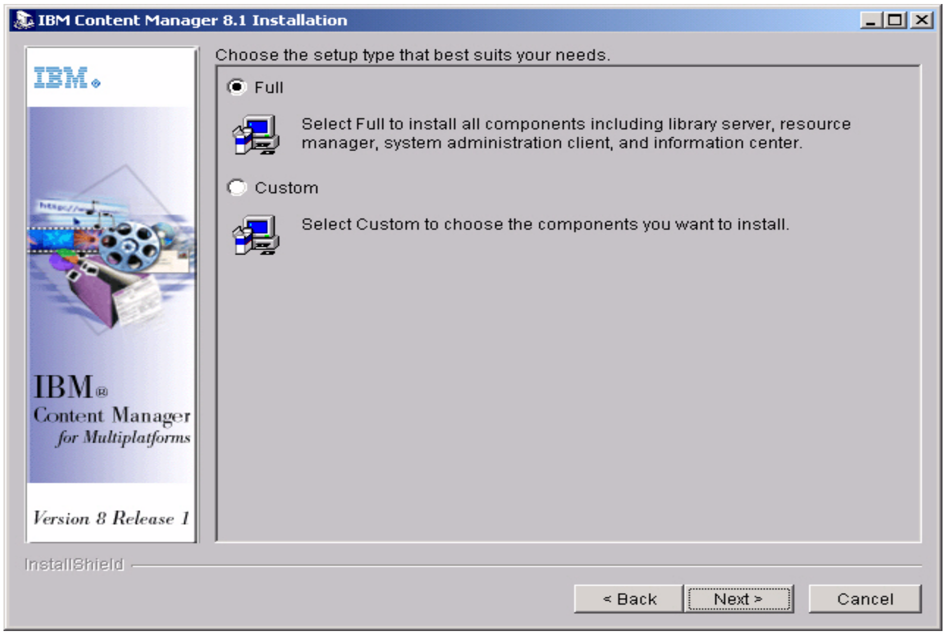
Full

Select **Full** if you want to install all of the Content Manager components on this same workstation:

- Library Server
- Resource Manager
- System Administration Client
- Information Center

Custom

Select **Custom** if you want to select which component(s) to install on this workstation.



IBM Content Manager 8.1 Installation

Choose the setup type that best suits your needs.

● Full

Select Full to install all components including library server, resource manager, system administration client, and information center.

○ Custom

Select Custom to choose the components you want to install.

Figure 3–7 *Choose Setup Screen*

5. ___ Choose to perform a **Full** install. This will install the Library Server, Resource Manager, System Administration Client, and Information Center. Select **Next** to continue.

6. ___ You may see a warning message indicating that a *Secured Sockets Layer (SSL) was not found.* Select **OK** to continue. You will configure SSL after the installation.

7. ___ If prompted to stop the WebSphere Application Server, choose **YES**. In order for the install program to automatically deploy the Resource Manager servlets, the application server **must** be stopped. (If you choose NO, then the Resource Manager servlets would have to be deployed manually.

Note: These manual steps are documented in the publication entitled *Planning and Installing Your Content Management System* (GC27-1332).

Configure Library Server

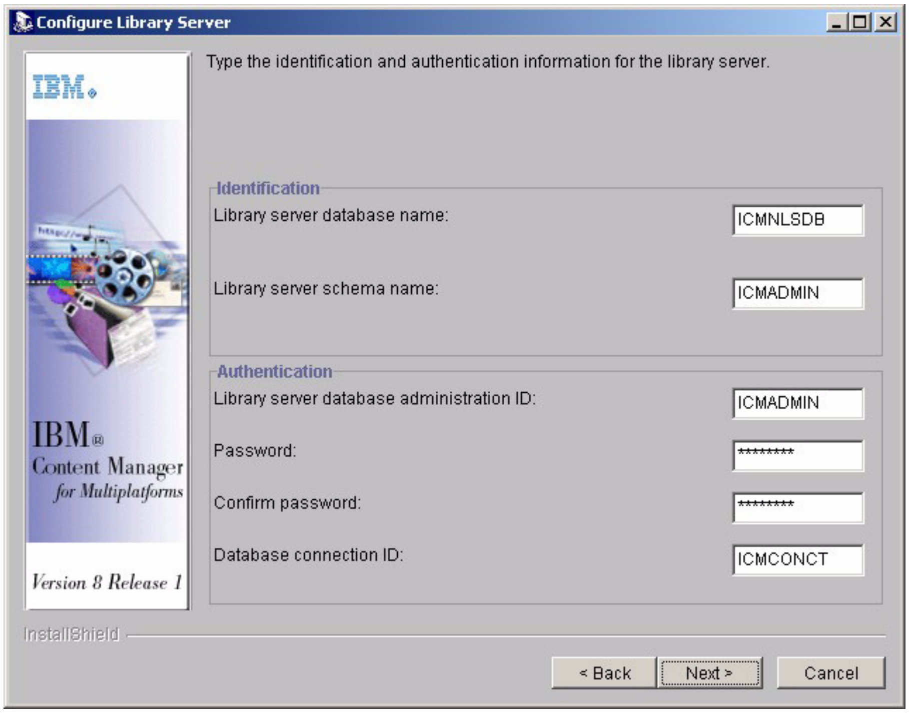
When you install the Library Server component, you must enter some information to configure your Library Server database (see Table 3–1 and Figure 3–8).

Table 3–1 *Library Server Configuration*

Install Information	Description	Default Name
Library Server Database Name	The Name of the Library Server Database	`ICMNLSDB`
Library Server Schema Name	The Library Server Database Schema Name	`ICMADMIN`
Library Server Database Administration ID	Administration ID for the Library Server [1]	`ICMADMIN`
Password	Password for the Library Server Administration ID[1]	`<password>`
Database Connection ID	Database Connection ID[2]	`ICMCONCT`

Notes:

1. This is the administration system user ID that you created before beginning the install process.
2. This is the database connection system user ID that you created before beginning the install process.



Type the identification and authentication information for the library server.

Identification

Library server database name: ICMNLSDB

Library server schema name: ICMADMIN

Authentication

Library server database administration ID: ICMADMIN

Password: *********

Confirm password: *********

Database connection ID: ICMCONCT

Figure 3–8 *Configure the Library Server*

8. ___ At the **Configure Library Server** screen (see Figure 3–8), enter the password for the *icmadmin* system user ID. Accept the remaining default values, and select **Next** to continue.

Note: The installation program checks to see if a Content Manager Library Server database or an EIP system administration database exist on this workstation.

If a database with the same name already exists, choose one of the following options:

- If the database is a Content Manager Library Server database, you are asked if you want to overwrite the existing database, keep it, or type in another name.
- If the database is an EIP system administration database, the installation program will configure the database so that both Content Manager and EIP could use it.

By creating a shared database for the Content Manager Library Server and EIP, you only need to maintain one set of access control privileges. Furthermore, any user IDs you create can be shared by both Content Manager and EIP. (In the previous version, Content Manager and EIP existed as two separate databases, therefore you had to maintain two sets of user IDs and access control privileges.)

Note: If you choose to recreate a Content Manager database that is also shared with the EIP, you will lose your EIP data.

Configure Library Server Options

Select the Library Server options for your installation (see Table 3–2 and Figure 3–9).

Table 3–2 *Library Server Configuration Options*

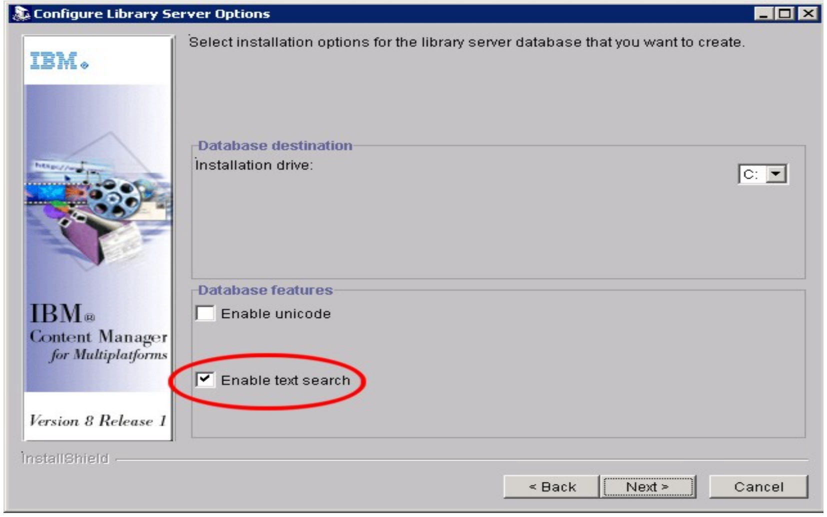
Install Information	Description	Default Name
Installation Drive (dropdown list of available choices)	The location of your Library Server Database	C:
Enable Unicode (check box)	Check this box to Enable Unicode	(Not checked/NO)
Enable Text Search (check box)	Check this box to enable the text search feature[1]	(Checked/YES)

Notes:

1. You must have the Text Information Extender (TIE) installed to use Text Search. If TIE is not installed, this check box is disabled.

2. You can install the TIE at any time after the Content Manager installation, but then you must manually enable the library database for text search.

Tip: Keep the Library Server database separate from the Resource Manager database for faster access. For even faster access, place the Library Server database on a dedicated drive.



Configure Library Server Options

Select installation options for the library server database that you want to create.

Database destination

Installation drive: C:

Database features

□ Enable unicode

☑ Enable text search

Figure 3–9 *Library Server Options*

9. ___ Choose **Enable text search** (see Figure 3–9).

Leave the database destination drive as **C**. This specifies the location of the Library Server DB2 database (not the actual Library Server program files). For production systems, you may want to place the Library Server database on its own drive (to allow for speed and a dedicated space for database growth).

10. ___ Select **Next** to continue.

Configure Resource Manager Server

When you install the Resource Manager component, you must enter the identification and authentication information for your Resource Manager (see Table 3–3 and Figure 3–10 on page 76).

Table 3–3 *Resource Manager Configuration*

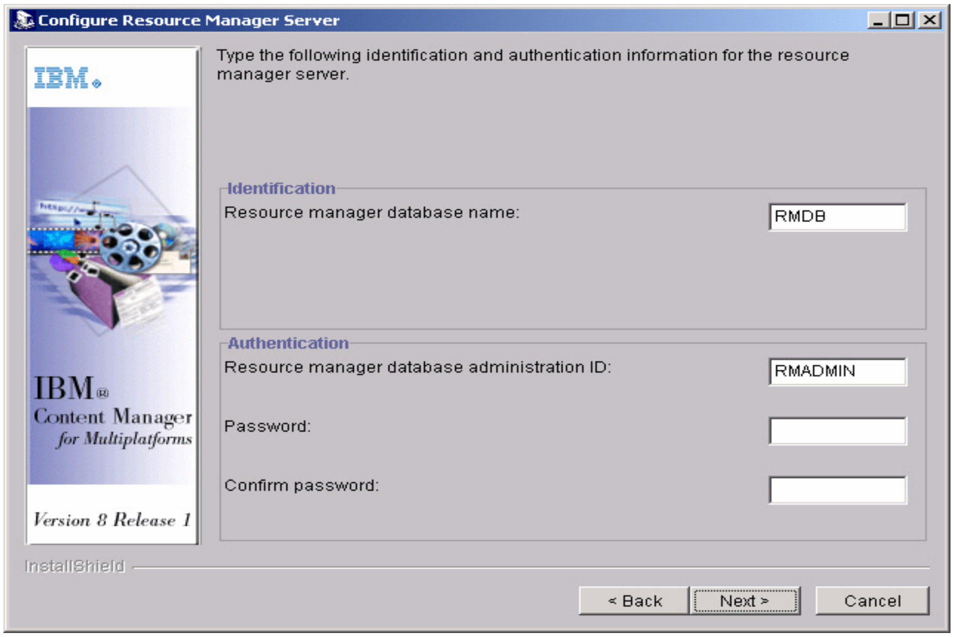
Install Information	Description	Default Name
Resource Manager Database Name	The Name of the Resource Manager Database	RMDB

Table 3–3 *Resource Manager Configuration*

Install Information	Description	Default Name
Resource Manager Database Administration ID	Administration ID for the Resource Manager [1]	`RMADMIN`
Password (two fields)	Password for the Resource Manager Administration ID[1]	`<password>`

Notes:

1. This is the Administration system user ID that you created before beginning the install process.



Configure Resource Manager Server
IBM.
IBM® Content Manager for Multiplatforms
Version 8 Release 1
InstallShield
< Back
Next >
Cancel

Type the following identification and authentication information for the resource manager server.

Identification

Resource manager database name: RMDB

Authentication

Resource manager database administration ID: RMADMIN

Password:

Confirm password:

Figure 3–10 *Resource Manager Identification and Authentication*

11. ___ At the **Configure Resource Manager Server** screen (see Figure 3–10), enter the password for the *rmadmin* system user ID. Accept the remaining default values, and select **Next** to continue.

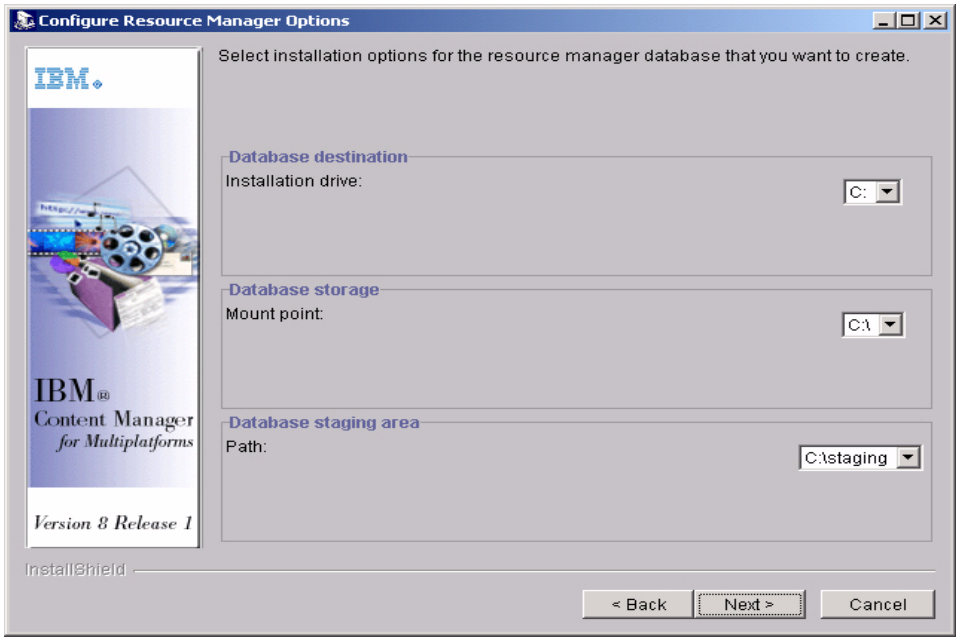
Note: The installation program checks to see if a Resource Manager database with the same name that you entered already exists. If the Resource Manager database already exists, you are asked if you want to overwrite the existing database, keep it, or type in another name.

Configure Resource Manager Server Options

Now you must enter your information for the Resource Manager database location, storage drive, and staging area path (see Table 3–4 and Figure 3–11 on page 78).

Table 3–4 *Resource Manager Server Options*

Install Information	Description	Default Name
Installation Drive (dropdown list of available choices)	The drive location of the Resource Manager Database	`C:\`
Mount Point (drop-down list of available choices)	Path to the drive used for storing objects	`C:\`
Staging Area Path	Path to the drive used for storing objects for LAN Cache or TSM objects	`C:\staging`



Select installation options for the resource manager database that you want to create.

Database destination

Installation drive: C:

Database storage

Mount point: C:\

Database staging area

Path: C:\staging

Figure 3–11 *Resource Manager Server Options*

12. ___ Accept the default Resource Manager Options (see Figure 3–11), and select **Next** to continue.

The *database destination drive* specifies the location of the Resource Manager DB2 database (not the actual Resource Manager program files). For production systems, you may want to place the Resource Manager database on its own drive (to allow for speed and a dedicated space for database growth).

The *mount point drive* specifies the default storage location of objects that are imported into this Resource Manager server. For production systems, it is **recommended** that the default storage location and the Resource Manager database be kept on separate drives.

The *staging area* is used as a cache for objects that are retrieved from optical storage (via the Tivoli Storage Manager).

Resource Manager with WebSphere Application Server

Identify the application server that your Resource Manager will use (see Table 3–5 and Figure 3–12).

Table 3–5 *Deploying the Resource Manager*

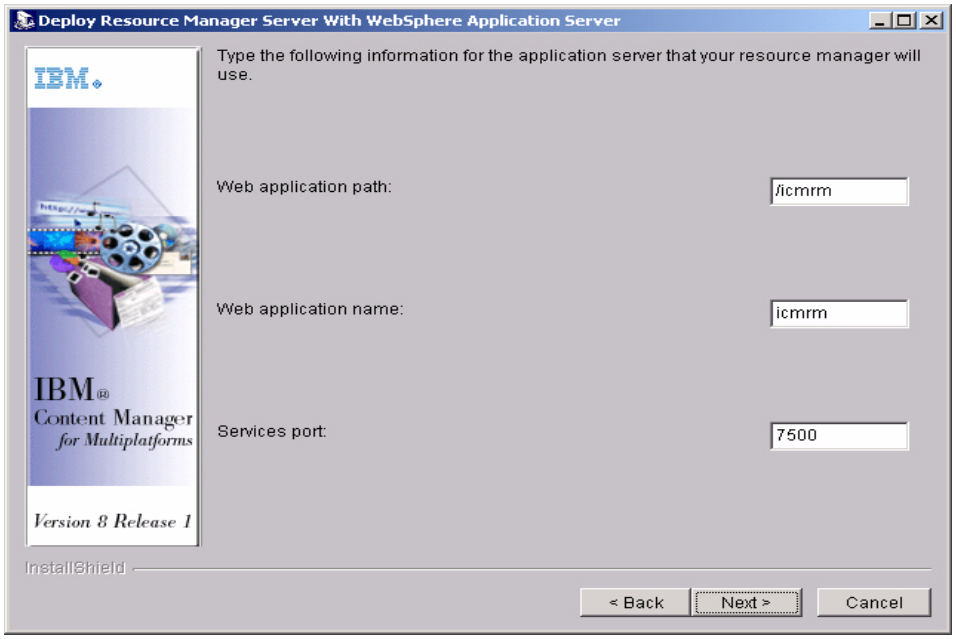
Install Information	Description	Default Name
Web Application Path	The context root of the Resource Manager web application	`/icmrm`
Web Application name	The name of the Web Application	`icmrm`
Services Port	Enter a port number (the first of four numbers) to be used for Resource Manager components: - Migrator - Purger - Stager - Replicator	`7500`[1,2].

Note:

1. You can enter a port number other than the recommended default number. However, it must be the first number of four available contiguous port numbers.

2. Installation will save port values in the services file.

   Windows systems: /winnt/system32/etc/drivers/services
   AIX systems: /etc/services



Type the following information for the application server that your resource manager will use.

Web application path: /icmrm

Web application name: icmrm

Services port: 7500

Figure 3–12 *Resource Manager Application Server*

13. ___ Accept the default deployment options for the Resource Manager, and select **Next** to continue.

The Resource Manager uses five ports (the specified services port plus the next four consecutive ports). For example, if port 7500 is specified, then ports 7501, 7502, 7503, and 7504 must also be available. The install program will add an entry into the `\winnt\system32\drivers\etc\services` file to have these ports reserved. By default, these ports are used for the following Resource Manager services (see Table 3–6).

Table 3–6 *Resource Manager Service Ports*

Port	Resource Manager Service
7500	Migrator
7501	Purger
7502	Replicator
7503	Stager
7504	Async Recovery

Configure System Administration Client

When you install the System Administration Client component, enter the appropriate information into the following fields to configure your System Administration Client (see Table 3–7).

Table 3–7 *Configure System Administration Client*

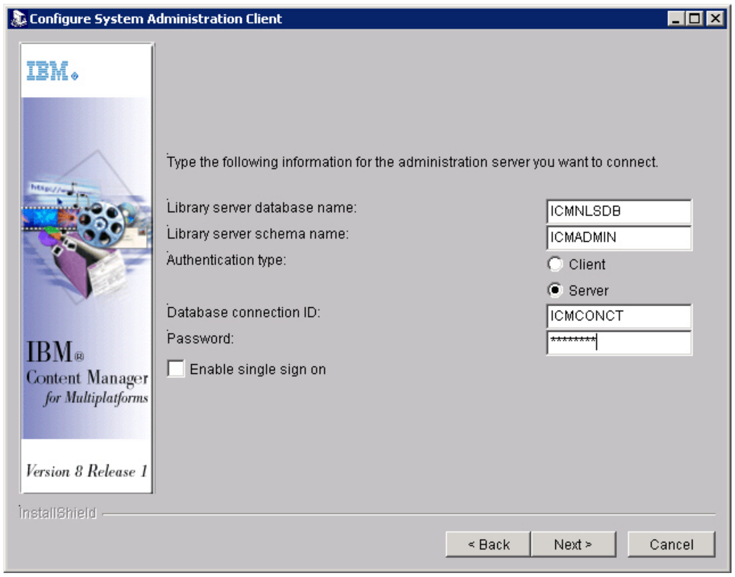
Install Information	Description	Default Name
Library Server Database Name	The Name of the Library Server Database	ICMNLSDB
Library Server Schema Name	The Library Server Schema Name	ICMADMIN
Authentication Type	DB2 database manager authentication[1]: Should match the settings on your DB2 server	Server
Database Connection ID	Database Connection ID[2]	ICMCONCT
Password (two fields)	Enter the Password for your Database Connection ID[2]	<password>
Enable Single Sign On (check box)	Check this box if you want to enable the Single Sign On option[3]	(Not checked/NO)

Client/Server Notes:

1. This is the setting that your DB2 administrator chose when configuring the DB2 database. For a detailed description of the differences between these two authentication types, refer to the section entitled *Database Connections* at the beginning of this chapter.

2. This is the database connection system user ID that you created before beginning the install process. The database data connection ID and password areas are only enabled for the Server authentication type.

3. The Enable single sign on option is enabled only if you selected the Client authentication type.



Type the following information for the administration server you want to connect.

Library server database name: ICMNLSDB

Library server schema name: ICMADMIN

Authentication type: ○ Client ● Server

Database connection ID: ICMCONCT

Password: ********

□ Enable single sign on

Figure 3–13 *Configure System Administration Client*

14. ___ At the **Configure System Administration Client** screen (see Figure 3–13), enter the **password** for the *icmconct* system user ID. Accept the remaining default values and select **Next** to continue.

The authentication type is directly related to the DB2 UDB database manager authentication. The default authentication type is *server*. However, if you want to enable the single sign-on feature, client authentication must be used. (For the purpose of this exercise, leave the authentication type as **server**.)

Location of System Configuration Information

You must indicate where your system configuration information is located for this system. The system configuration files consist of a set of **.ini* and **.property* files which contain configuration information. One important configuration file is *cmbicmsrvs.ini*. This file has an entry for each Content Manager Version 8.1 Library Server, and is used by the System Administration Client to determine what servers are available.

Note: The *cmbicmsrvs.ini* file serves the same function as the *frnolint.tbl* (network table) file did in Content Manager Version 7.

Because this is a new installation, you should choose **local** so that the configuration files can be generated. Once the configuration files are created, they can be published on a shared directory or on a web server. New Content Manager Client installations could then use these existing configuration files. By using a common set of configuration files, enterprise wide updates can easily be made.

Due to the flexibility of Content Manager you have a number of options:

a. You can store system configuration information on this Local workstation, or you can use system configuration that is stored on a Remote workstation or that you plan to store there later. *(During this installation you are indicating where the configuration information will be at the time that it is needed by the system.)*

b. You can use system configuration information on an HTTP web server.

c. You can use configuration information on an LDAP server (which may or may not exist at this time, but will exist at the time that it is needed by the system).

You can use a combination of any of the above three options.

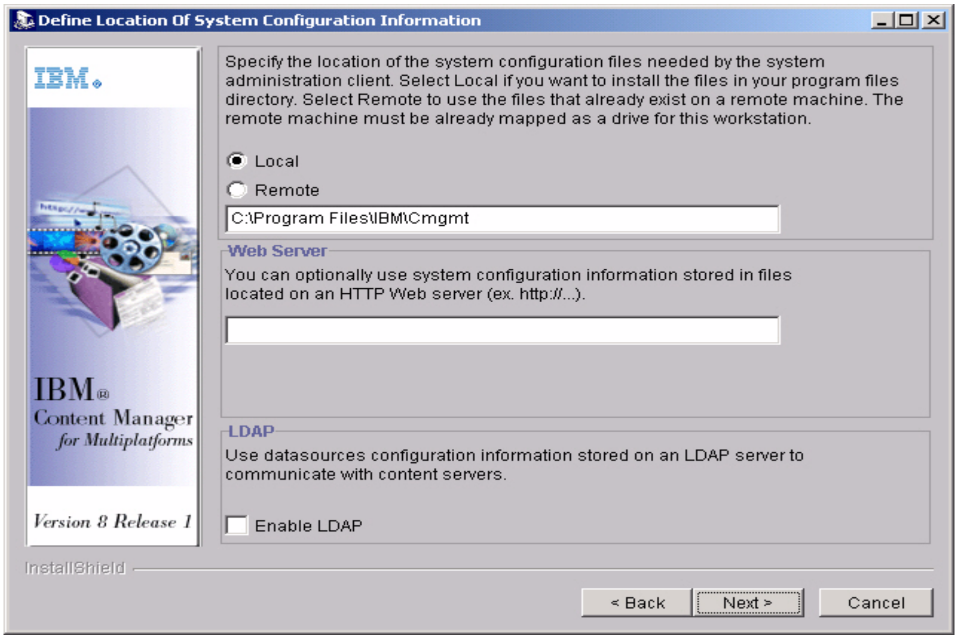
What you choose depends on what you are trying to do with your servers, and how you want users to have access to various components of your system (see Table 3–8 and Figure 3–14 on page 84).

Table 3–8 *System Configuration Information*

Install Information	Description	Default Name
Select Local or Remote	Select Local to install the configuration information on this workstation. Select Remote if your configuration information is (or will be) located on a remote, networked-mapped workstation.	Local
(Area for entering the location of the remote configuration information file)	For Remote, enter the file path name where your configuration information is located.	`<path>`

Table 3–8 *System Configuration Information*

Install Information	Description	Default Name
Web Server	Area for entering a valid URL address of the remote web server. (in the form of: http://...)	(no default)
Enable LDAP (check box)	Check this box if you would like to use datasources configuration information stored on an LDAP server. .	(Not checked/ NO)


Define Location Of System Configuration Information
IBM
IBM Content Manager for Multiplatforms
Version 8 Release 1
InstallShield
< Back
Next >
Cancel

Specify the location of the system configuration files needed by the system administration client. Select Local if you want to install the files in your program files directory. Select Remote to use the files that already exist on a remote machine. The remote machine must be already mapped as a drive for this workstation.

● Local

○ Remote

C:\Program Files\IBM\Cmgmt

Web Server

You can optionally use system configuration information stored in files located on an HTTP Web server (ex. http://...).

LDAP

Use datasources configuration information stored on an LDAP server to communicate with content servers.

□ Enable LDAP

Figure 3–14 *System Configuration Screen*

15. ___ Accept **Local** as the location of the system configuration files (see Figure 3–14), and leave the *LDAP* option **unchecked**. Select **Next** to continue.

Connect Library Server To Resource Manager

When you connect a Library Server to a Resource Manager, you **must** enter information about the Resource Manager that the Library Server needs to connect to it (see Table 3–9).

Table 3–9 *Connect Library Server to Resource Manager*

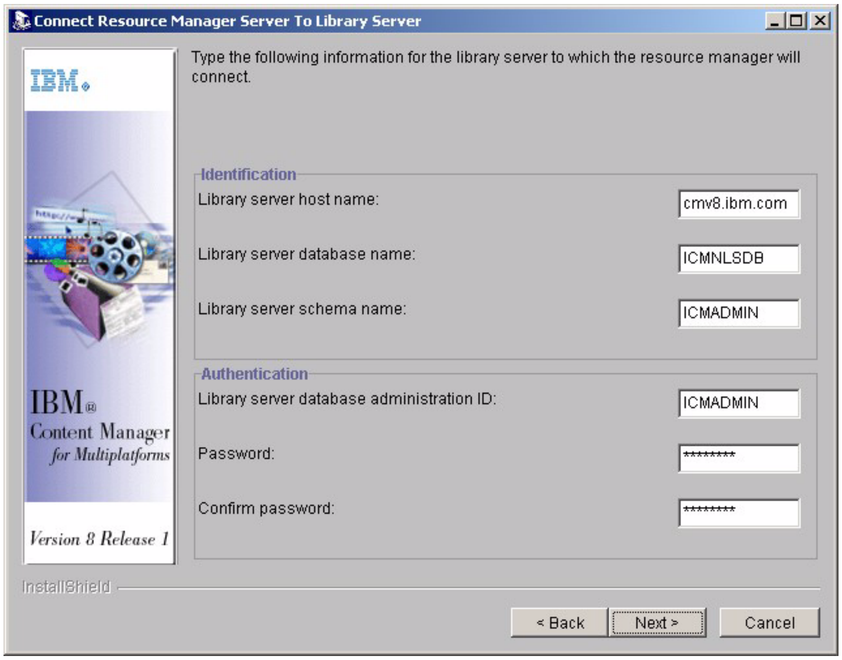
Install Information	Description	Default Name
Resource Manager server host name	The host name of the workstation that contains the Resource Manager.	`<host name>`
Resource Manager database name	The name of the Resource Manager database.	`RMDB`
Web application port	The Port number used to access the Resource Manager. This is usually the port number of the Web Server that is configured for use with WebSphere.	80
Secure Web application port (HTTPS)	The Port number that the system administration client should use to communicate with the Resource Manager. This should be the port SSL is configured on.	443
Web application path	The context root of the Resource Manager web application.	`/icmrm`
Resource Manager database operating system (drop-down list of available choices)	The operating system of the workstation where the Resource Manager is located.	`<platform>`

Table 3–9 *Connect Library Server to Resource Manager*

Install Information	Description	Default Name
Token duration (hours)	Tokens are created by the Library Server when clients need to store/retrieve documents to/from a Resource Manager. This sets the amount of time (hours) that a token remains valid. After the token expires, it cannot be reused, and the client must request a new token from the Library Server. (This can be modified later with the system administration client.)	48

16. ___ At the **Connect Library Server to Resource Manager Server** screen (see Figure 3–15), enter the *fully qualified hostname* of this workstation, and select **Next** to accept the default settings.

Note: One way to validate the hostname value is to go to a command window, and *ping* it. If the *ping* fails, try using the TCP/IP address. If the TCP/IP address works, then you should specify the TCP/IP address as the *hostname* value.



Connect Resource Manager Server To Library Server

Type the following information for the library server to which the resource manager will connect.

Identification

Library server host name: cmv8.ibm.com

Library server database name: ICMNLSDB

Library server schema name: ICMADMIN

Authentication

Library server database administration ID: ICMADMIN

Password: ********

Confirm password: ********

Figure 3–15 *Connect Library Server to Resource Manager Server*

Configure Components for LDAP

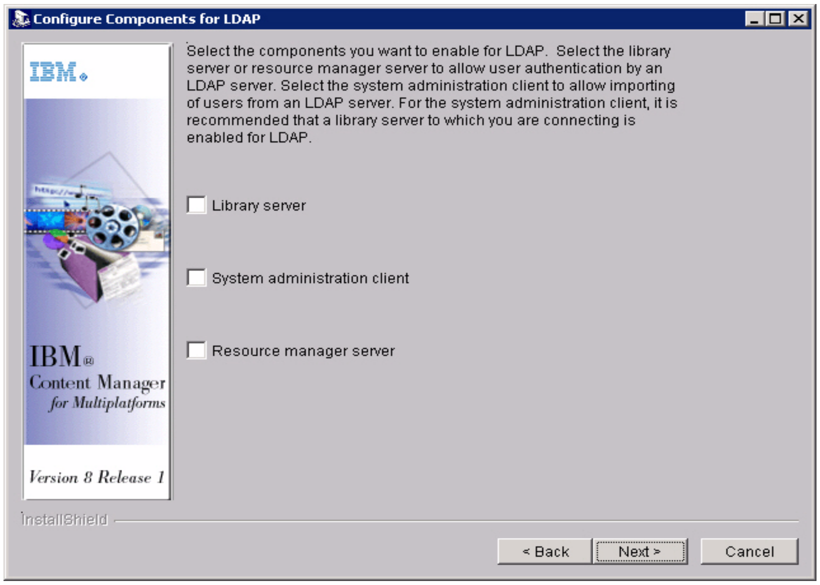
Select the components that you want to enable for LDAP (see Table 3–10 and Figure 3–16 on page 88).

Table 3–10 *Configure Components for LDAP*

Install Information	Description	Default Name
Library Server (check box)	Check this box to allow user authentication for the Library Server by an LDAP server.	(not checked/NO)
System Administration Client (check box)	Check this box to allow importing of users from an LDAP server.	(not checked/NO)

Table 3–10 *Configure Components for LDAP*

Install Information	Description	Default Name
Resource Manager Server (check box)	Check this box to allow user authentication for the Resource Manager by an LDAP server.	(not checked/NO)



Configure Components for LDAP

Select the components you want to enable for LDAP. Select the library server or resource manager server to allow user authentication by an LDAP server. Select the system administration client to allow importing of users from an LDAP server. For the system administration client, it is recommended that a library server to which you are connecting is enabled for LDAP.

☐ Library server

☐ System administration client

☐ Resource manager server

Figure 3–16 *Configure Components for LDAP*

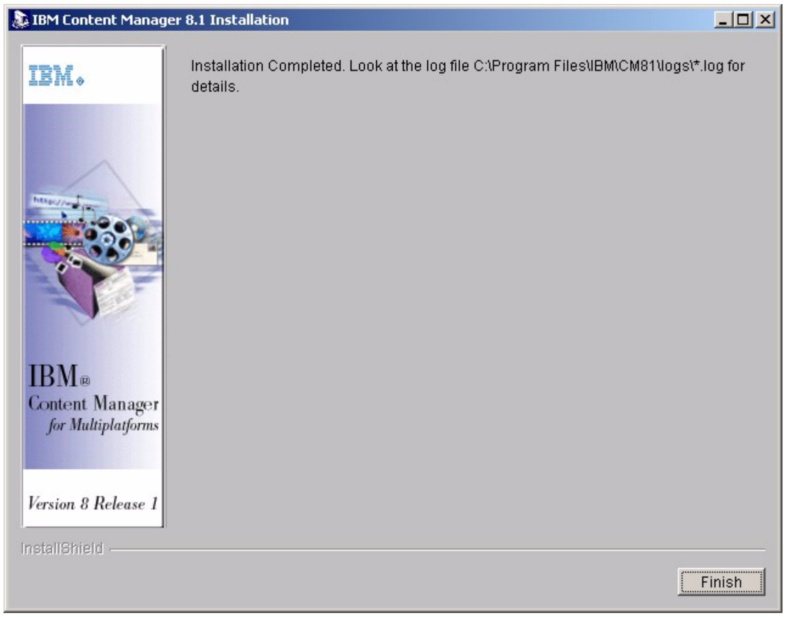
17. ___ At the **Configure Components for LDAP** screen, leave **all** components **unchecked** and select **Next** to continue.

Verify Install Location and Component Selection

Verify that the installation information is correct. (If any parameters are incorrect, you can return to previous screens by using the **Back** button.)

18. ___ Select **Next** to begin the process of copying files. During this time, product files are copied, and the server databases will be created. (If you are asked to replace any existing files, select **Yes to All**.)

The **Start Copying Files** screen opens and you will soon see a message that installation has been successful, (see Figure 3–17).

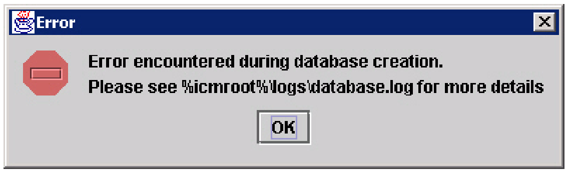

IBM Content Manager 8.1 Installation
IBM.
IBM® Content Manager for Multiplatforms
Version 8 Release 1
InstallShield
Finish

Installation Completed. Look at the log file C:\Program Files\IBM\CM81\logs\*.log for details.

Figure 3–17 *Successful Installation*

If you received an error message during installation, such as what is shown in Figure 3–18, you can view the log files in your `%ICMROOT%/logs` directory. (By default, `%ICMROOT%` is `C:\Program Files\IBM\CM81`)

This particular error message indicates that an error occurred while creating the server database(s). You must review the database creation log files (which are described in the next section), to determine why the error occurred.



Error encountered during database creation.
Please see %icmroot%\logs\database.log for more details

Figure 3–18 *Failed to Create Server Database*

19. ___ Select **Finish** to complete and exit the installation program.

Review Installation Logs

Before continuing, you should always check the installation log files for any errors that may have occurred. Usually, errors can be corrected without having to do a complete reinstall.

1. ___ Go to `C:\Program Files\IBM\CM81\logs`. Notice that each installation step creates its own log file. Also note that some messages may be nothing more than a warning message (which usually requires no action on your part).

2. ___ To check that the Library Server database was created successfully, open *icmcrlsdb.log*. Scan through this file, and make sure all the commands were completed successfully. Pay particular attention to the *CREATE TABLESPACE* commands. An unsuccessful return code usually means *icmadmin* was not assigned to the Administrator's system group.

You can easily recreate the Library Server database by going to **Start | Programs | IBM Content Manager for Multiplatforms | Library Server Database Install**.

3. ___ To check that the Resource Manager server database was created successfully, open *icmcrrmdb.log*. Scan through this file, and make sure all the commands were completed successfully. For example, a common mistake is to forget to assign *rmadmin* to the system Administrator's group. This error would result in the following message: *RMADMIN does not have the privilege to perform operation*.

You can easily recreate the Resource Manager database by going to **Start | Programs | IBM Content Manager for Multiplatforms | Resource Manager Database Install**.

Note: The existence of database.log usually means that the access modules for system defined item types did not get generated successfully. Misconfigured LIB, PATH, and / or INCLUDE environment variables will cause this problem.

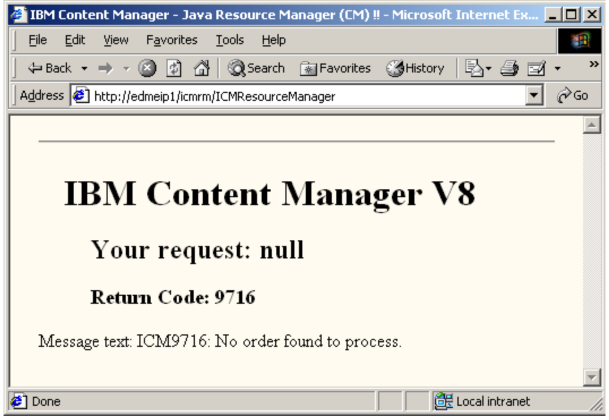
4. ___ Look over the remaining log files for any errors. The existence of *database.log* usually means that the access modules for system defined item types did not get generated successfully. For example, you will usually see the following text in this file:

```
Error creating item types: ,
exception=com.ibm.mm.sdk.common.DKUsageError: DGL3711A: Error
occurred while compiling the component type;  ICM7307: An
```

```
error occurred while creating the DLL to access a component
table.  Review the server log for the name of the access
module, and then review the corresponding ICMxxxxx.TX files
(for example, ICMVxxxx.tx3) for details. (STATE) : [LS RC =
7307, LS reasonCode = 2]
```

This is usually caused by incorrect environment variables (review the section entitled *Configuring Environment Variables* in Chapter 4) or not having the DB2 Application Development Client installed.

5. ___ To test the deployment of the Resource Manager servlets, open a web browser and go to http://<hostname>/icmrm/ICMResourceManager. You should see a page similar to the example in Figure 3–19.


IBM Content Manager - Java Resource Manager (CM) !! - Microsoft Internet Ex...
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://edmeip1/icmrm/ICMResourceManager
Go
Done
Local intranet

IBM Content Manager V8

Your request: null

Return Code: 9716

Message text: ICM9716: No order found to process.

Figure 3–19 *Testing Resource Manager Deployment*

If you get an error message, make sure that both *WebSphere* and the *icmrm* web application are running. Also regenerate the web server plug-in.

Note: You will not be able to store objects / blobs if the Resource Manager is not operating properly.

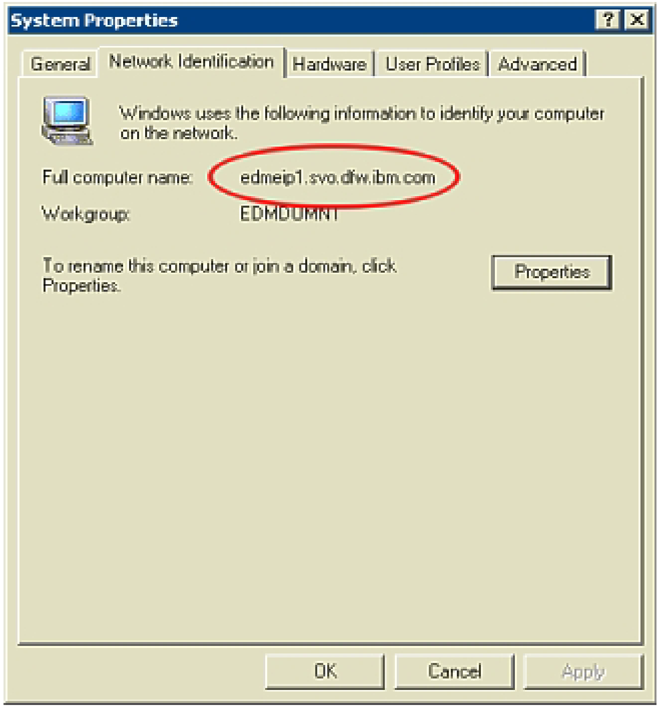
6. ___ To test the Library Server, start the Content Manager System Administration client (located in **Start | Programs | IBM Content Manager for Multiplatforms**), and login as *icmadmin* (password is *password*). If you get an error message, review the Library Server log file (by default it is located at `C:\ICMSERVER.LOG`). If the login is successful, exit the System Administration Client (use the client in the following chapter exercises).

Configure Secured Sockets Layer (SSL)

Secured Sockets Layer (SSL) is used to ensure secure communication between two machines, and is required when performing Resource Manager configuration. In other words, in order to access a Resource Manager via the System Administration client, SSL must be properly configured.

> **Note:** SSL is required to configure the Resource Manager via the System Administration Client. However, it is NOT required to store and retrieve documents.

Before beginning the SSL configuration on Windows, you must have a valid TCP/IP configuration. It is also **important** that your **full computer name be the fully qualified hostname** of your workstation. To check your full computer name, go to the *Windows Control Panel*, open *System*, and choose the *Network Identification* tab (see Figure 3–20).



Windows uses the following information to identify your computer on the network.

Full computer name: edmeip1.svo.dfw.ibm.com

Workgroup: EDMDUMNT

To rename this computer or join a domain, click Properties.

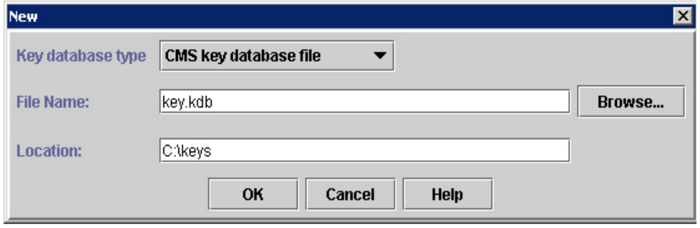
Figure 3–20 *System Properties Screen*

The following is a concise set of steps for configuring SSL with IBM HTTP Server. A more in-depth discussion of SSL, and detailed configuration steps can be found in Chapter 18 of the publication entitled *Planning and Installing Your Content Management System* (GC27-1332).

1. ___ Create a folder on drive C called **keys**. You will be saving the key database files in this directory.

2. ___ Start the *Key Management Utility* by selecting **Start | Programs | IBM HTTP Server | Start Key Management Utility**.

3. ___ From the menu bar, select **Key Database File**, **New**. At the New Key Database screen, (see Figure 3–21), specify the location to be `C:\keys`. Select **OK** to save the new key database.



New

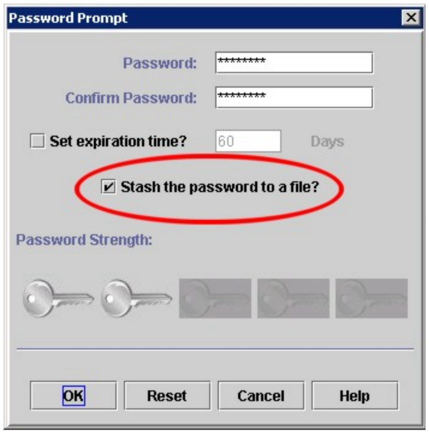
Key database type: CMS key database file

File Name: key.kdb

Location: C:\keys

Figure 3–21 *New Key Database*

4. ___ At the *Password Prompt* screen, (see Figure 3–22), enter ***password*** as the password. (For a production environment, you will want to choose a password that contains both letters and numbers for higher security.)



Password Prompt

Password: ********

Confirm Password: ********

☐ Set expiration time? 60 Days

☑ Stash the password to a file?

Password Strength:

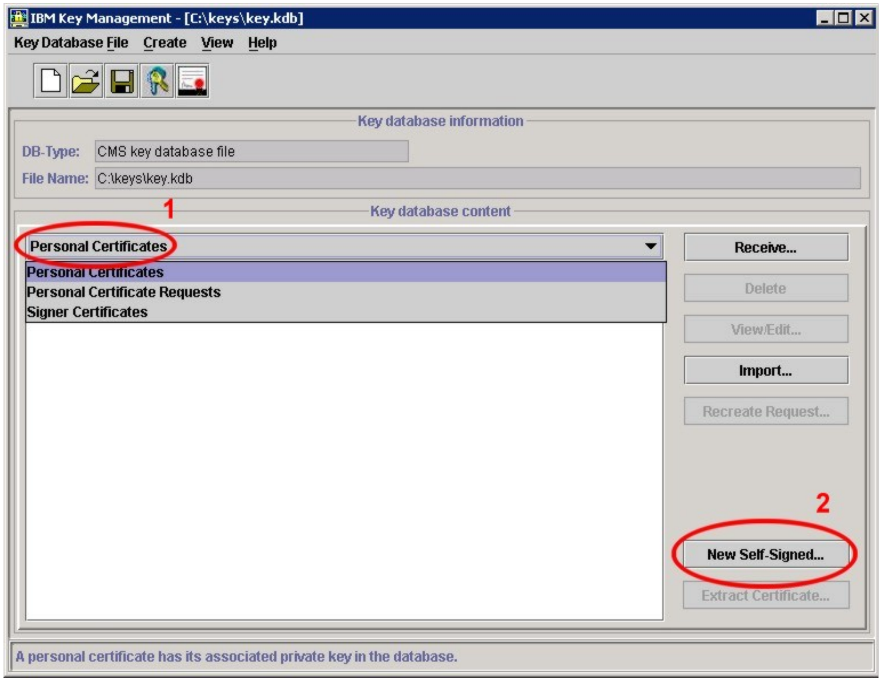
Figure 3–22 *Password Prompt Screen*

5. ___ Place a checkmark on the box labeled **stash the password to a file** and select **OK** to save.

6. ___ Create a new self-signed certificate by selecting **Personal Certificates** from the drop down combo box and then selecting **New Self-Signed** (Figure 3–23).

7. ___ On the *Create New Self-Signed Certificate* screen (see Figure 3–24), enter **icmrm** as the key label. Enter the **fully qualified hostname** of the web server, which in this case, is your workstation (for example, *cmv8pc.ibm.com*) as the common name. Enter a short descriptive name (for example, *IBM*) for your organization. Leave all other values at their default settings. Select **OK** to save.

8. ___ **Close** the *Key Management Utility* program.



IBM Key Management - [C:\keys\key.kdb]

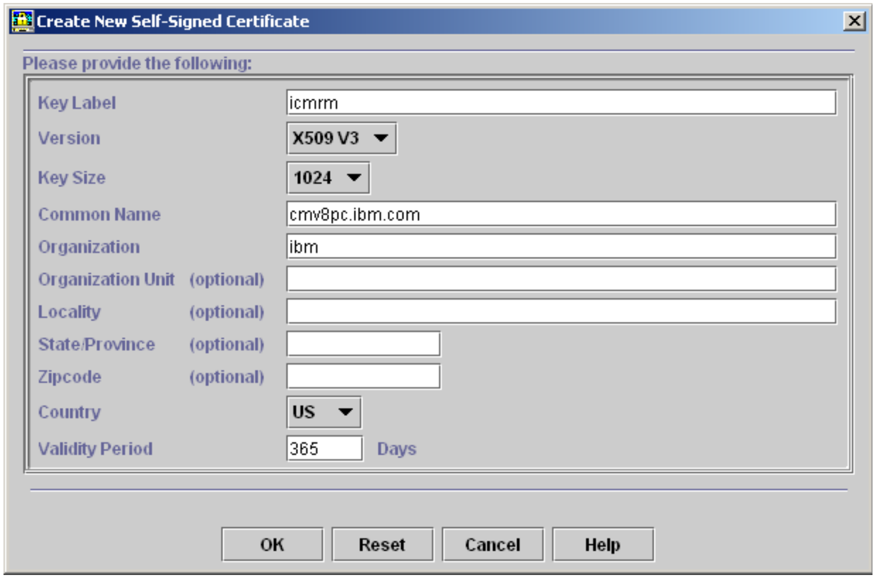
Key database information

DB-Type: CMS key database file

File Name: C:\keys\key.kdb

A personal certificate has its associated private key in the database.

Figure 3–23 *Selecting a New Self-Signed Certificate*



Create New Self-Signed Certificate

Please provide the following:

Key Label		icmrm
Version		X509 V3
Key Size		1024
Common Name		cmv8pc.ibm.com
Organization		ibm
Organization Unit	(optional)	
Locality	(optional)	
State/Province	(optional)	
Zipcode	(optional)	
Country		US
Validity Period		365 Days

Figure 3–24 *Creating a New Self-Signed Certificate*

At this point, you have created a key database file and a self-signed certificate. The next step is to configure the web server for SSL. Chapter 18 of the publication entitled *Planning and Installing Your Content Management System* (GC27-1332), contains detailed steps on how to use the IBM HTTP Server GUI for SSL configuration.

Instead of following the manual steps detailed in the Content Manager documentation, you may elect to copy and paste the information described in the following step. (Following the instructions in Chapter 18 of the publication entitled *Planning and Installing Your Content Management System* (GC27-1332), or the following three steps will result in the same outcome.)

Installing Content Manager

9. ___ Open `C:\IBM HTTP Server\conf\httpd.conf` in Notepad. Copy the following lines to the **end** of `httpd.conf`:

```
AddModule mod_ibm_afpa.c

AddModule mod_so.c

AddModule mod_mime.c
AddModule mod_access.c
AddModule mod_auth.c
AddModule mod_negotiation.c
AddModule mod_include.c
AddModule mod_autoindex.c
AddModule mod_dir.c
AddModule mod_cgi.c
AddModule mod_userdir.c
AddModule mod_alias.c
AddModule mod_env.c
AddModule mod_log_config.c
AddModule mod_asis.c
AddModule mod_imap.c
AddModule mod_actions.c
AddModule mod_setenvif.c
AddModule mod_isapi.c
AddModule mod_rewrite.c
LoadModule  ibm_ssl_module  modules/IBMModuleSSL128.dll
Listen 443
<VirtualHost cmv8pc.ibm.com:443>
DocumentRoot  "c:/ibm http server/htdocs"
SSLEnable
Keyfile c:\keys\key.kdb
SSLV2Timeout 100
SSLV3Timeout 1000
SSLClientAuth none
SSLServerCert  icmrm
SSLCipherSpec 39
SSLCipherSpec 3A
SSLCipherSpec 62
SSLCipherSpec 64
</VirtualHost>
```

10. ___ Make sure the VirtualHost tag (shown above in bold) contains the correct fully qualified hostname.

11. ___ **Save** and **close** `httpd.conf`.

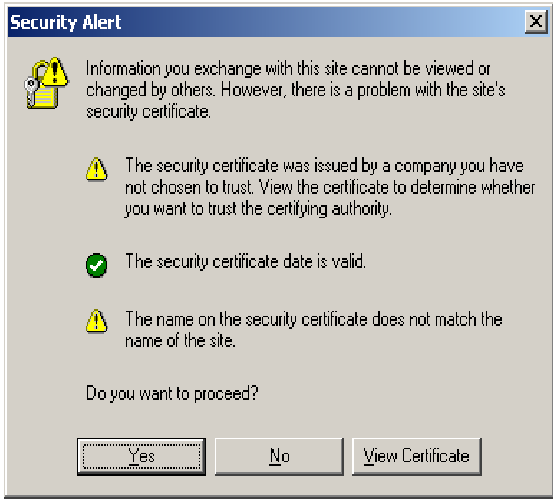
12. ___ Go to the **Windows Services** Control panel, and **restart** the service named *IBM HTTP Server*. (If the server does not start, then you have a syntax error in the httpd.conf file.)

13. ___ Open a web browser, and go to http://<hostname>, where <hostname> is the hostname of your machine. You should see the normal IBM HTTP Server welcome screen.

Next, test the SSL connection by going to https://<hostname>.

Note: SSL does not work with the *localhost* hostname. You must use the real <hostname>.)

If SSL was configured properly, you should see a window asking you to accept a personal-signed certificate, (see Figure 3–25). After selecting **YES**, the IBM HTTP Server welcome screen should appear.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

Figure 3–25 *Prompt to Accept Self-Signed Certificate*

If the SSL certificate prompt does not appear, check the log files in `C:\IBM HTTP Server\logs` for any error messages.

14. ___ Test the SSL connection to the Resource Manager Server by opening a web browser and going to https://<hostname>/icmrm/ICMResourceManager. You should see a web page similar to the example of Figure 3–19 on page 91.

Note: If using WebSphere AE, you must configure WebSphere to accept requests on port 443. This procedure is documented in Chapter 18 of the publication entitled *Planning and Installing Your Content Management System* (GC27-1332).

At this point, you have successfully installed the Content Manager Version 8.1 servers and the System Administration Client. You have also configured SSL so the Resource Manager configuration could be performed.

Installing Content Manager Client for Windows

It is not necessary to uninstall an earlier version of the Client for Windows program before you begin. Previous versions of the client use environment variables that begin with *FRN* and use the C Folder Manager APIs for communication. The new Version 8.1 client uses environment variables that begin with *ICM* and *CMB*, and uses the EIP V8.1 C++ object oriented APIs for communication.

Note: A Content Manager Version 7 client cannot communicate with a Content Manager Version 8.1 server. Likewise, a Content Manager Version 8.1 client cannot communicate with a Content Manager Version 7 server.

Before You Begin

Before you begin the installation, you need to plan for and obtain information that you will need during the Client for Windows installation. You need to know where your *Initialization* (configuration) files will be located.

- Remote *http* location
- Remote *mapped* network location
- Local workstation

These initialization files were created by the Content Manager Server installation. In an enterprise environment, you would want to place these initialization files on a shared resource (such as a web server or network drive). This allows all Content Manager clients to use the same set of files, and allows for easier maintenance.

If you specify that the initialization files will be located on a local workstation, and if the installation program detects that the files are not yet created, you will be prompted to supply the following information so that the installation program can create the initialization files for you (see Table 3–11).

Table 3–11 *Manually Creating Initializing Files*

Parameter	Description	Default Name
Datastore alias name	Name of Library Server database	ICMNLSDB
DB2 user ID	Database connection system user ID used to connect to Library Server database.	icmconct
DB2 Password	Password of database connection user ID	password
DB2 Schema Name	Schema name of database	ICMADMIN
Database Location	Specifies whether the Library Server database is on this workstation or on a remote workstation	This computer (local)
Database Authentication	DB2 database manager authentication. Should match the settings on your DB2 server	Server
Single Sign-on	Check this box if you want to enable the Single Sign-on option	not checked

If you specified that the Library Server database location is remote (on another machine), then you must also supply information so that the database can be cataloged on the local machine, (see Table 3–12 on page 101).

Table 3–12 *Remote Database Catalog Information*

Parameter	Description	Default Name
Hostname of Database Server	The hostname of the workstation that has the Library Server database	<hostname of Library Server>
Port Number	Port number of DB2 instance	50000
Remote Database Name	Name of database on the remote database server	ICMNLSDB
Operating System of Server	System platform of the remote database server	WinNT/2000

For more information about initialization (*ini*) files, see the step entitled, *Location of System Configuration Information* in the Content Manager Server Installation section of this chapter.

Beginning the Installation

To begin the installation, shut down any open Windows applications, including antivirus software.

1. ___ Insert the Client for Windows CD into your CD-ROM drive.
2. ___ Select the language that you want to use during the installation program.
3. ___ Enter your customer information, and select **Next** to continue.
4. ___ Accept the default destination directory and select **Next** to continue.

Note: If you have a previous version of the Client for Windows on this workstation, the installation program does not use that location for the program. This allows you to have both a Version 8.1 and a Version 7.2 Client installed and operable.

5. ___ Choose **Typical** setup and select **Next** to continue.

Typical *(Recommended)*

This selection does not install all possible components. The following components are **not installed**:

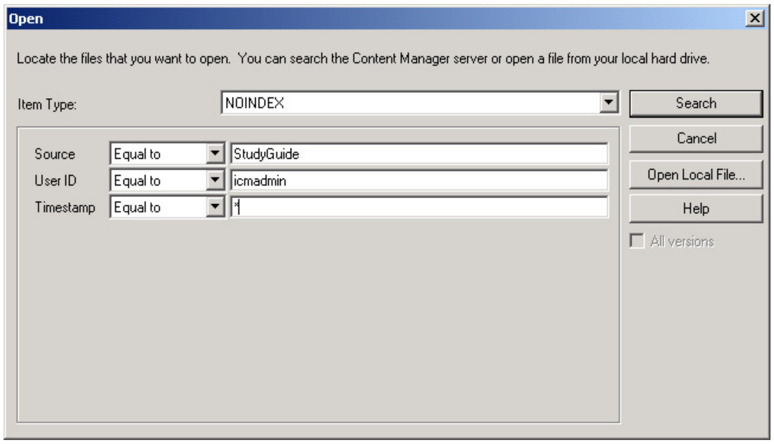
- Scanner support *(a sub-component under Client Application)*
- Additional languages
- ODMA

Custom

This allows you to select additional components that are not installed during a *Typical* installation.

ODMA

Install ODMA support if you want to be able to access documents stored in a Content Manager system directly from specific workstation applications. By using an ODMA aware desktop application (such as Microsoft Word), when you choose to open a file, you can search for a specific document within your Content Management system. The ODMA architecture will transparently checkout the document, and retrieve it to your workstation for editing. Likewise, when you choose to save the document, you will be prompted for attribute information for the selected item type. The ODMA architecture will also transparently store the document into the Content Manager system. (Figure 3–26 and Figure 3–27 on page 103 depict the ODMA open and save dialogs.)

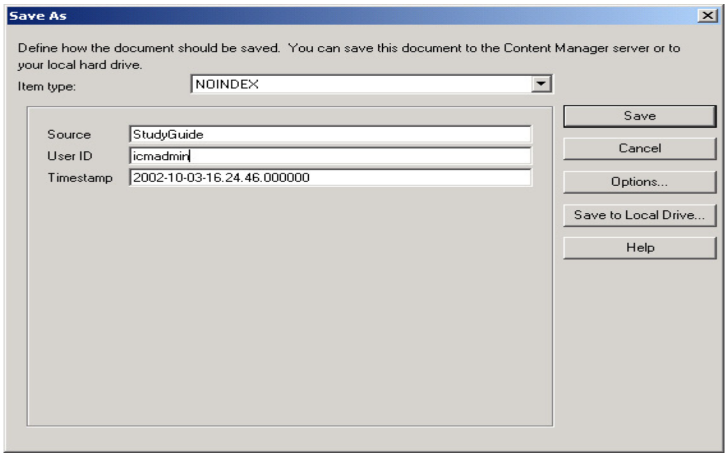


Locate the files that you want to open. You can search the Content Manager server or open a file from your local hard drive.

Item Type: NOINDEX

Source Equal to StudyGuide
User ID Equal to icmadmin
Timestamp Equal to *

Figure 3–26 *ODMA Open Dialog*



Define how the document should be saved. You can save this document to the Content Manager server or to your local hard drive.

Item type: NOINDEX

Source StudyGuide
User ID icmadmin
Timestamp 2002-10-03-16.24.46.000000

Figure 3–27 *ODMA Save Dialog*

ODMA installs only in the same language that the install program runs in. At the time of this writing however, **ODMA is not translated** into the following languages (codes):

- Czech Republic (CZE)
- Danish (DAN)
- Hebrew (HEB)
- Hungarian (HUN)
- Norwegian Bokmal (NOR)
- Russian (RUS)
- Slovakian (SKY)
- Swedish (SVE)

Note: You must be using an ODMA aware client (i.e. Microsoft Word) in order to utilize the ODMA function of Content Manager. Be aware that most desktop applications are not ODMA aware.

6. ___ Because the Content Manager initialization files are not published on a web server, there is no REMOTE location to specify. Leave the text field blank and select **Next** to continue.
7. ___ Accept the default **LOCAL** location of Content Manager initialization files and select **Next** to continue.

When everything is on a single machine, specifying the LOCAL location of the initialization files is the obvious choice. However, when installing the Client for Windows on multiple machines, specifying a REMOTE location for the initialization files would be more efficient. This would allow all your clients to share a single copy of the **.ini* and **.properties* files. To specify a remote location, you **must** first publish these initialization files on a web server.

8. ___ Select **Install** to begin the process of copying files.

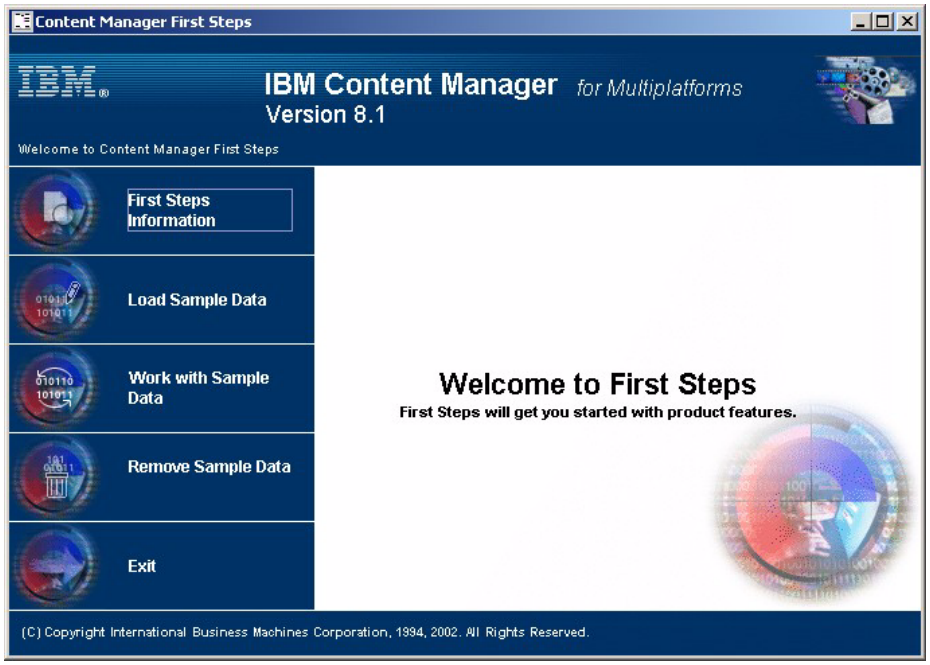
Note: Unlike Content Manager Version 7, Content Manager Version 8.1 has no communication isolator. Instead, when a client connects to the Library Server, it is making a database connection to the *ICMNLSDB* database. This architecture allows Content Manager to leverage the communication protocol of the underlying database software.

In order to make a connection to the DB2 database, the client must have a DB2 client installed on it. The Client for Windows installation program will automatically install the DB2 Run-Time Client if it is missing, and will then catalog the Library Server database as a datasource on the client machine.

9. ___ Select **Finish** to complete and **Exit** the installation program.

Content Manager First Steps

Content Manager First Steps (see Figure 3–28) is installed along with the System Administration Client, and can be run by selecting **Start | IBM | IBM Content Manager for Multiplatforms V8.1 | First Steps**.



Welcome to Content Manager First Steps

Welcome to First Steps

First Steps will get you started with product features.

(C) Copyright International Business Machines Corporation, 1994, 2002. All Rights Reserved.

Figure 3–28 *Content Manager First Steps Welcome Screen*

The First Steps wizard allows you to create a sample document model and load sample content into your Content Manager system. It will create five different item types:

- An auto claim form
- An adjuster report
- A police report
- An insurance policy
- Photos/videos of damaged automobiles

Note: Before loading data with First Steps, it is strongly advised that you first test your installation by creating a sample item type and importing a document into the system. This would allow you to resolve any problems before running the automated First Steps scripts.

You can use the Content Manager System Administration Client to explore the sample document model. You can also use the Client for Windows to view the sample content.

Important Files You Should Know

In order to become proficient with the Content Manager Version 8.1 system, you must be familiar with certain key files which are created by the installation program. Some of these files are used by the APIs and clients, and also control the level of logging/tracing. By understanding where these files are, and what they do, you will be better equipped to troubleshoot problems.

Note: You are strongly encouraged to become familiar with these installation log files and initialization files. Open each one in notepad to see what it contains.

Installation Logs

During the installation, various *log* files will be created by different components. These log files are vital in resolving installation errors and/or validating the database creation process.

Table 3–13 and Table 3–14 list the locations and descriptions of the various Content Manager installation log files.

Table 3–13 *Content Manager UNIX Install Log Files*

Filename	Description
$ICMROOT/logs/cm81install.log	Contains install program messages
$ICMROOT/config/icmcrlsdb.log	Library Server database creation
$ICMROOT/config/icmcrrmdb.log	Resource Manager database creation
$ICMROOT/logs/database.log	Created when access modules could not be generated
AIX: $ICMROOT is /usr/lpp/icm	
SUN: $ICMROOT is /opt/IBMicm	

Table 3–14 *Content Manager Windows Install Log Files*

Filename	Description
$ICMROOT\logs\cm81install.log	Contains install program messages
$ICMROOT\logs\icmcrlsdb.log	Library Server database creation
$ICMROOT\logs\icmcrrmdb.log	Resource Manager database creation
$ICMROOT\logs\database.log	Created when access modules could not be generated
$ICMROOT\logs\rmconfig.log	Logs Resource Manager deployment and configuration

$ICMROOT is `C:\Program Files\IBM\CM81` by default

Initialization Files

Initialization files are used by the APIs and clients to communicate with servers and control the level of logging/tracing. Table 3–15 lists the important initialization files and a description of what each one is used for. These files are located in a directory specified by `%CMCOMMON%`, which by default is as follows:

- Windows: C:\Program Files\IBM\CMGMT
- AIX: /usr/lpp/cmb/cmgmt
- SUN: /opt/IBMcmb/cmgmt

Table 3–15 *Important Initialization Files*

Filename	Used By	Description
cmbcmenv.properties	CM & EIP	Information telling CM/EIP where to look for other configuration files. (For example, locally, remote machine, web server, or LDAP)
cmbicmsrvs.ini	CM & EIP	Contains a list of all available CMV8 Library Servers. This file performs the same function as the frnolint.tbl network table did in CMV7.

Table 3–15 *Important Initialization Files*

Filename	Used By	Description
cmbds.ini	EIP	Contains a list of all available EIPV8 servers.
cmbicmenv.ini	CM & EIP	Contains encrypted database connection user ID and password for CMV8 Library Servers.
cmbfedenv.ini	EIP	Contains encrypted database connection user ID and password for EIPV8 servers.
cmbcs.ini	CM & EIP	Determines whether or not a RMI server should be used for the various connectors.
cmbsvcs.ini	EIP	Determines whether or not a RMI server should be used for information mining and workflow.
cmbclient.ini	EIP	RMI server information for the connectors.
cmbsvclient.ini	EIP	RMI server information for information mining and workflow services.
cmadmin.properties	CM & EIP	Used by the system administration client to determine if CM, EIP, or both CM and EIP are installed. This file is located in `%CMSYSADMIN%`, which is `C:\ProgramFiles\IBM\CMGMT\admin\common` by default.
icmrm.properties	CM	Bootstrap/Initialization information for Resource Manager.

Summary

In this chapter you have reviewed the process of installing Content Manager on the Windows operating system. You learned that when connecting to a Content Manager Library Server, there are two different connections: a physical connection to the database, and a logical connection to the Content Manager Library Server. The APIs must first be able to connect to the Library Server database for example, *ICMNLSDB*. Once the connection to the database is made, the APIs will query the user table (which contains the Content Manager user IDs) to validate the client user ID and password.

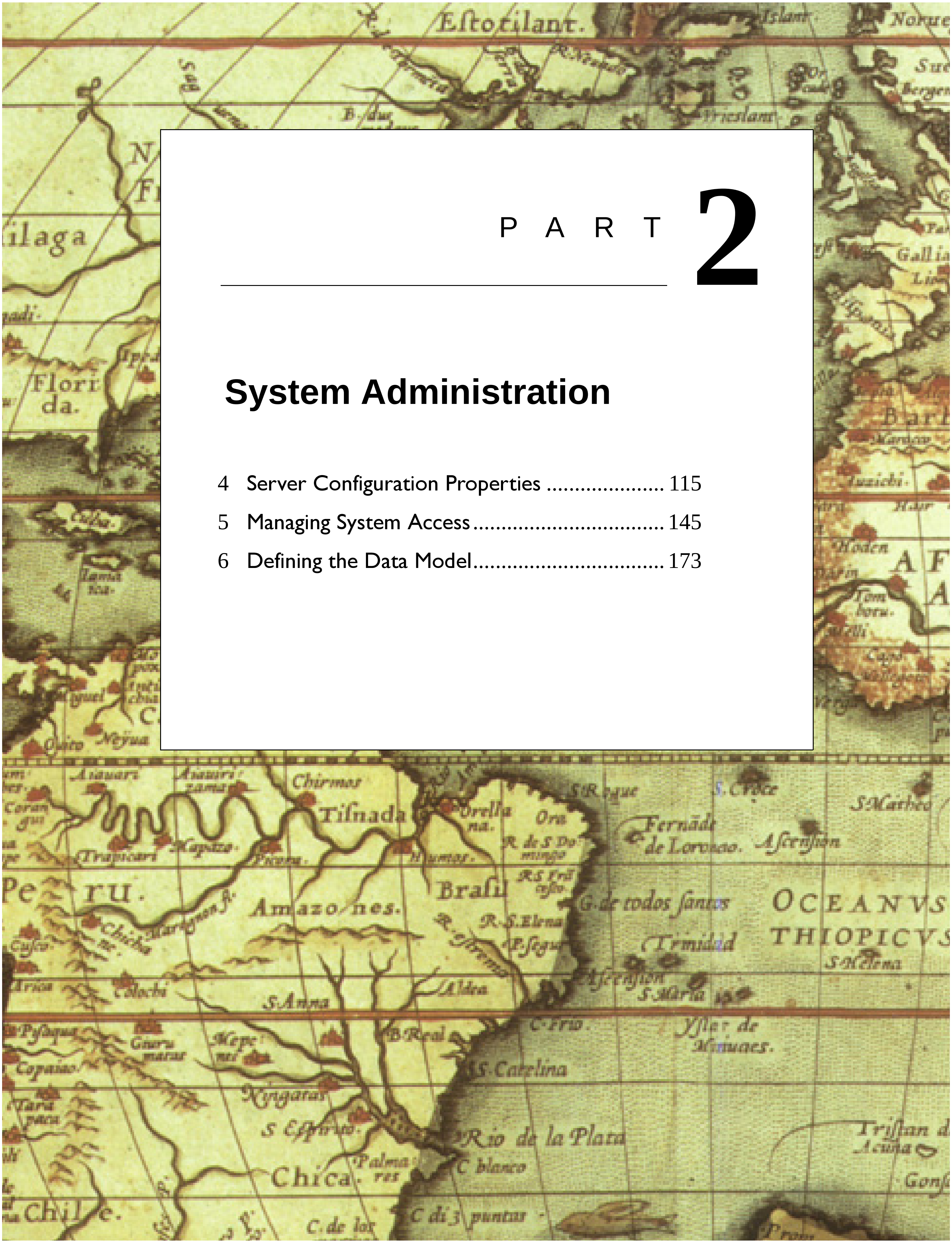
The physical connection to the database is authenticated by the database manager (DB2 UDB), and therefore requires that a system user ID be created. Instead of having to have a system user ID for every Content Manager user ID, a shared database connection user ID (*icmconct*) can be used.

You became familiar with the installation process for the servers and clients. You also learned that initialization files contain the information needed by clients in order to connect to the Content Manager servers. Of particular interest was the cmbicmsrvs.ini, which contains an entry for each Library Server in your enterprise. These initialization files can be placed on a shared resource (such as a web server or network drive) so that all clients can use a common set of files.

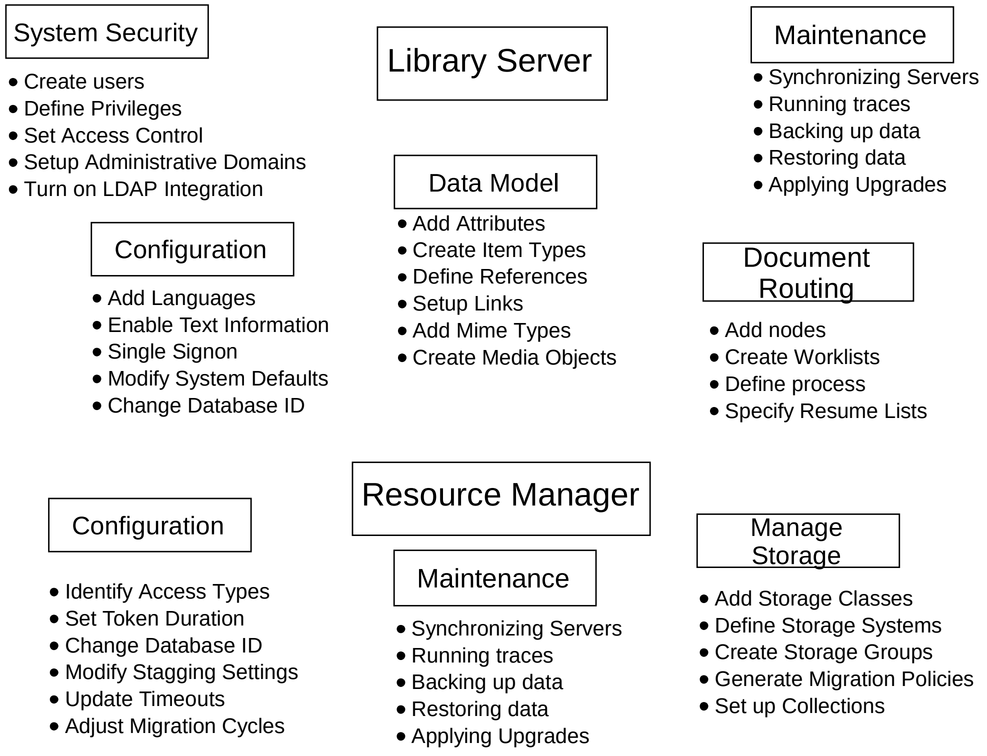
The Content Manager First Steps wizard is a Java application installed with the Windows System Administration Client and can be used to become familiar with the new Content Manager document model. Lastly, the location of key files created by the installation program was described.

PART 2

System Administration



With Content Manager and the prerequisite software installed the system configuration options need to be modified to reflect the desired operational system. This includes determining whether to use LDAP, Administrative Domains, and other features of Content Manager. Before content can be loaded into Content Manager, the system Data Model and User Authorizations need to be defined. In addition, if Document Routing is going to used, it might be best to define the various processes prior to users storing information. This section will introduce you to the Content Manager System Administration Client and its various options for administering the IBM Content Manager system. This includes Library and Resource Manager server properties, user authorization and access control, building a data model, and defining document routing processes. To support you in this, on-line help is provided on each screen in the Content Manger System Administration Client for answers, as well as step-by-step instructions to complete specific tasks. In addition, you should review the *System Administration Guide (SC27-1335)*. The following picture summarizes administrative tasks that apply to the Content Manager system



Library Server

System Security

- Create users
- Define Privileges
- Set Access Control
- Setup Administrative Domains
- Turn on LDAP Integration

Configuration

- Add Languages
- Enable Text Information
- Single Signon
- Modify System Defaults
- Change Database ID

Data Model

- Add Attributes
- Create Item Types
- Define References
- Setup Links
- Add Mime Types
- Create Media Objects

Maintenance

- Synchronizing Servers
- Running traces
- Backing up data
- Restoring data
- Applying Upgrades

Document Routing

- Add nodes
- Create Worklists
- Define process
- Specify Resume Lists

Resource Manager

Configuration

- Identify Access Types
- Set Token Duration
- Change Database ID
- Modify Stagging Settings
- Update Timeouts
- Adjust Migration Cycles

Maintenance

- Synchronizing Servers
- Running traces
- Backing up data
- Restoring data
- Applying Upgrades

Manage Storage

- Add Storage Classes
- Define Storage Systems
- Create Storage Groups
- Generate Migration Policies
- Set up Collections

CHAPTER 4

Server Configuration Properties

- System Administration Client
- Library Server Configuration
- Resource Manager Properties
- Content Manager Trace Levels
- Language Definitions

This chapter assumes you are the system administrator who is responsible for setting up and maintaining the Content Manager system for your enterprise. At this point, you must have already installed or migrated your system to IBM Content Manager version 8.1. Use the Installing Content Manager section of this study guide or see the document, *Planning and Installing Your Content Management System* (GC27-1332); if you have not completed these tasks.

This chapter provides conceptual information and steps for understanding the Content Manager System Administrative Client and the various configuration options that can be modified for the Library and Resource Manager servers. This section does not cover the System Managed Storage features of the Resource Manager. These topics are covered in a later section dealing with Tivoli Storage Manager integration.

System Administration Client Overview

IBM Content Manager version 8.1 introduces many new enhancements and modifications to the System Administration client such as the following:

- Object Server renamed to Resource Manager
- Users and Groups are now under Authentication
- Access Control Lists and Privilege Sets are under Authorization
- Fileroom is now called Data Modeling
- Index Classes are now Item Types
- LDAP integration screens have been added
- Text Information Extender integration screens have been added
- Administrative Domains have been added

Content Manager (CM) and the Enterprise Information Portal (EIP) use the same System Administration Client. While in the System Administration Client, you can switch between the Content Manager and EIP server definitions. When Content Manager is installed the default tables that are needed for EIP are also added to the system. Using the DB2 Control Window to view the Content Manager Library server database, you will see tables starting with *ICM* for Content Manager and those starting with *FA* used by the EIP or shared between Content Manager and EIP services. Therefore, the System Administration Client architecture is common between both products (see Figure 4–1 on page 117).

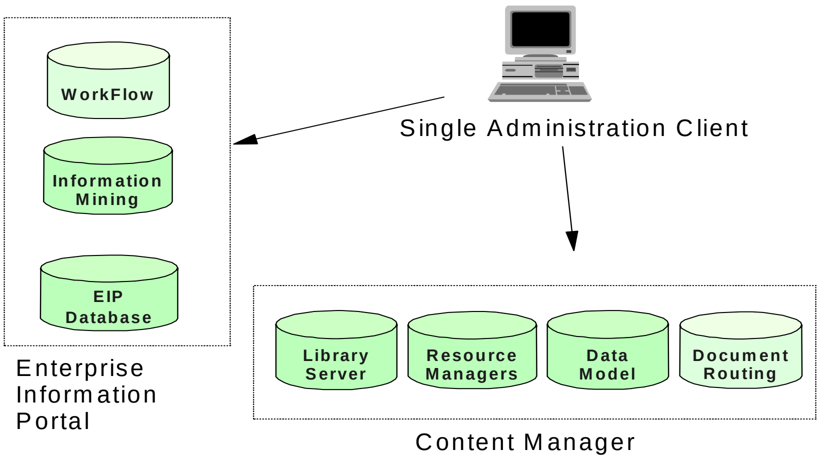


Figure 4–1 *Single Administration Across Multiple Products*

Along with the common architecture is the support for Content Manager and EIP servers running on different platforms (see Figure 4–2).

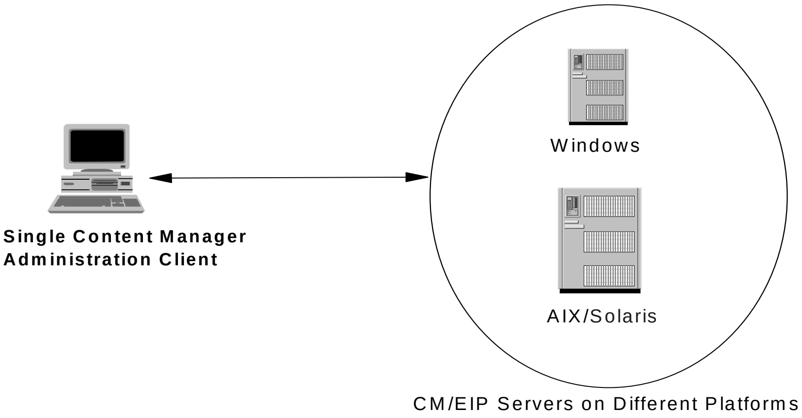

Single Content Manager Administration Client
Windows
AIX/Solaris
CM/EIP Servers on Different Platforms

Figure 4–2 *Single Administration Across Multiple Platforms*

Logging on to the System Administration Client

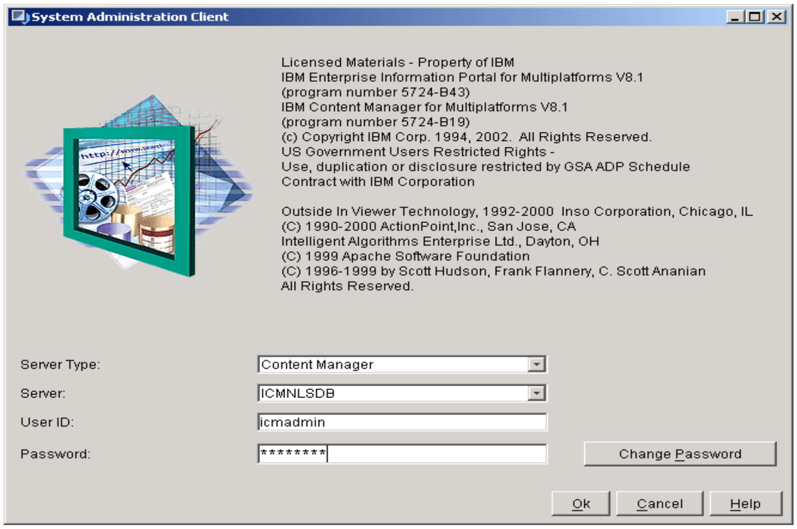
From the System Administration Client, you can access both the Content Manager and EIP system administration databases without having to log off and logon again. You can also start the System Administration Client from more than one location using the same user ID. You can start multiple clients from the same machine or different machines.

Note: You must be using a Library Server configuration that allows multiple logons.

1. ___ Start the *System Administration client* by selecting, **Start | Programs | IBM Content Manager for Multiplatforms V8.1 | System Administration**

2. ___ Specify the default user ID **ICMADMIN** and **password**.

Notice the logon screen in Figure 4–3 asks for a *Server Type* and *Server*. Accept the defaults shown on the screen. These fields are present because the same System Administrative Client is now used to manage both Content Manager and EIP. The server type represents the product and the server represents the database instance for the Content Manager Library Server or the EIP database.



Licensed Materials - Property of IBM
IBM Enterprise Information Portal for Multiplatforms V8.1
(program number 5724-B43)
IBM Content Manager for Multiplatforms V8.1
(program number 5724-B19)
(c) Copyright IBM Corp. 1994, 2002. All Rights Reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule
Contract with IBM Corporation

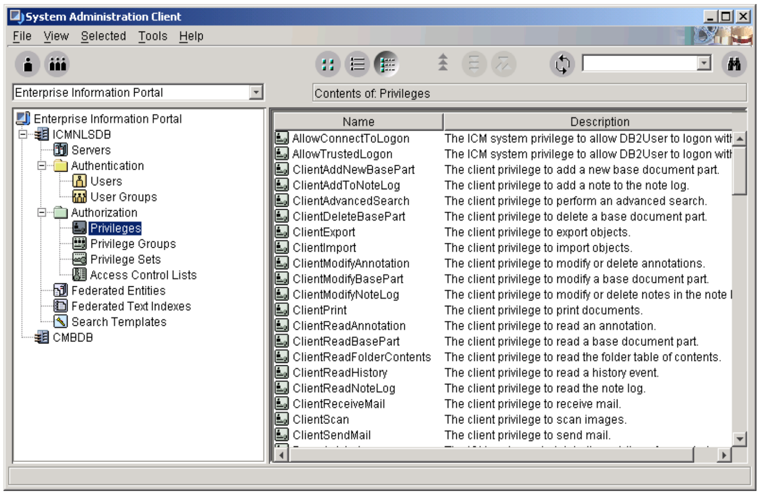
Outside In Viewer Technology, 1992-2000 Inso Corporation, Chicago, IL
(C) 1990-2000 ActionPoint,Inc., San Jose, CA
Intelligent Algorithms Enterprise Ltd., Dayton, OH
(C) 1999 Apache Software Foundation
(C) 1996-1999 by Scott Hudson, Frank Flannery, C. Scott Ananian
All Rights Reserved.

Server Type: Content Manager
Server: ICMNLSDB
User ID: icmadmin
Password: ********

Figure 4–3 *The System Administration Client Logon Screen*

3. ___ Press **OK** to logon and display the System Administration Client.

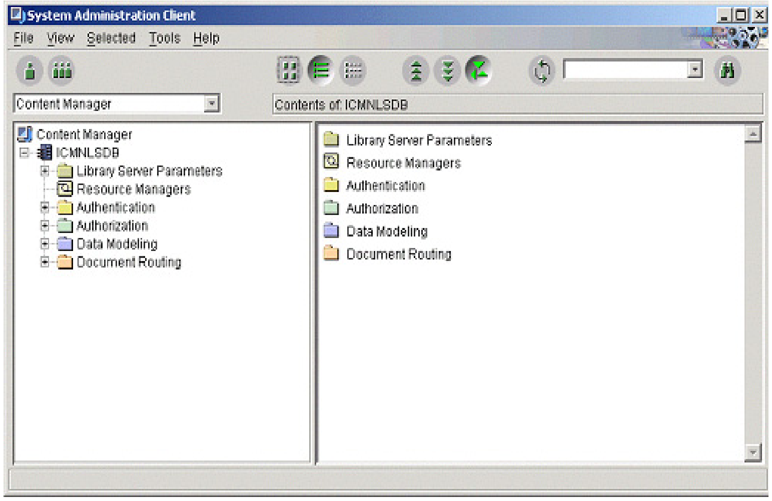
Figure 4–4 on page 119 shows an example of the System Administration Client screen for the EIP. Figure 4–5 on page 119 shows an example of the System Administration Client screen with the Content Manager view selected. This study guide covers the Content Manager tasks and will not go into detail on the EIP administration tasks. This is because the *IBM Certification Solutions Expert (CSE) - IBM Content Manager Version 8.1 Certification Exam 442* covers Content Manager and does not contain detailed questions content on the EIP database, server definitions, advanced workflow, or information mining.



Contents of: Privileges

Name	Description
AllowConnectToLogon	The ICM system privilege to allow DB2User to logon wit
AllowTrustedLogon	The ICM system privilege to allow DB2User to logon wit
ClientAddNewBasePart	The client privilege to add a new base document part.
ClientAddToNoteLog	The client privilege to add a note to the note log.
ClientAdvancedSearch	The client privilege to perform an advanced search.
ClientDeleteBasePart	The client privilege to delete a base document part.
ClientExport	The client privilege to export objects.
ClientImport	The client privilege to import objects.
ClientModifyAnnotation	The client privilege to modify or delete annotations.
ClientModifyBasePart	The client privilege to modify a base document part.
ClientModifyNoteLog	The client privilege to modify or delete notes in the note l
ClientPrint	The client privilege to print documents.
ClientReadAnnotation	The client privilege to read an annotation.
ClientReadBasePart	The client privilege to read a base document part.
ClientReadFolderContents	The client privilege to read the folder table of contents.
ClientReadHistory	The client privilege to read a history event.
ClientReadNoteLog	The client privilege to read the note log.
ClientReceiveMail	The client privilege to receive mail.
ClientScan	The client privilege to scan images.
ClientSendMail	The client privilege to send mail.

Figure 4–4 *EIP Administration Screen*



Contents of: ICMNLSDB

Figure 4–5 *Content Manager Administration Screen*

As the system administrator, you will use the Content Manager system administration areas listed in Table 4–1 to complete the setup of your system. (This table lists the different administrative areas within the System Administration Client.) This includes using the *authorization* area to define privilege sets for access to objects and then assigning privileges to users defined under the *authentication* area.

The *data modeling* area is a critical step in setting up the system. It is important to lay out the hierarchy of your data model prior to defining it in the system. Making decisions ahead of time as to the depth of the data model using child components, the expanse of the data model using links and references, and taking into account various restrictions like parts of the data model supported by the Content Manager clients, will allow you to define a model appropriate for current and future data needs.

Table 4–1 *Content Manager System Administration Areas*

Administration Areas	What is Covered
Library Server Parameters	Where one modifies the Library Server options like maximum logon attempts, password duration, maximum users, single sign on, enabling LDAP, enabling Text Information Extender, access control list system defaults, and setting the logging and trace levels.
Resource Managers	The properties for the Resource Manager allow one to set the user ID and password for the database connection. This is where the protocol and ports used by the WebSphere based Resource Manager are defined. The objects under Resource Manager allow one to setup the System Managed Storage options in Content Manager.
Administrative Domains	Added after Administrative Domains have been enabled on the system. Allows for the creation of different domains that the system administrator can assign to other administrators for management.
Authentication	Create user definitions and assign access rights. Also assign users to groups.
Authorization	Define Privilege Sets and Access Control Lists that define the access a user has to objects stored in the system.
Data Modeling	Where one defines the attributes, item types, references, links, MIME Types, and other information on how objects will be organized within the system.
Document Routing	Setup a Content Manager based workflow by creating work nodes, processes and work lists. This is separate from the Advanced Workflow that comes with Enterprise Information Portal.

Switching Product Views

In earlier versions of the Content Manager system, if you had Content Manager and EIP as part of your enterprise solution, you had to open two separate System Administration Clients. In version 8.1 and later, if you have both products installed, you can administer both systems from the same user interface. Switching from one system administration view to the other provides a convenient way to modify information that applies to both systems and fast access to either product.

To switch from one product to the other without logging off, go to the main system administration window and use the pull-down menu above the left pane. If the pull-down menu lists any product other than the one that you are currently using, you can switch to that product.

Switching Library Servers

If you plan to switch Library Servers while you are logged on to the System Administration Client, you must make sure that the server databases, where the Library Servers reside, are running. The Library Server is defined by its database, so the Library Server comes up and goes down with its associated database.

To switch Library Servers, select the Library Server that you want to work on in the left pane. Notice that the list of Resource Managers has changed accordingly (expand Resource Managers in the left pane of the System Administration Client main window). Resource Managers can only be associated to one Library Server, so each time you change Library Servers, you get access to a new list of Resource Managers.

Keyboard Access

You can use the keyboard to access all of the functions of the System Administration Client. In general, access from the keyboard follows many of the standard Microsoft guidelines. For example, you can open the File menu from the keyboard by holding down the **Alt** key and pressing **F**.

However, access from the keyboard differs from standard Microsoft guidelines in the following ways:

Access Keys, Tabbing, and Tables

Access keys are provided only for buttons and menu items. Press *Tab* to reach fields that do not have a shortcut key combination.

Within a table, the *Tab* key moves the cursor to the next cell. To move out of the table to the next field, hold down the **Ctrl** key and press **Tab**. When the cursor is within a table, pressing *Enter* is not equivalent to selecting *OK*; you must move out of the table first.

Menus

Pressing *Alt+Spacebar* does not open the Program menu from the left icon on the title bar of the Content Management System Administration window. Pressing *Shift+F10* does not open pop-up menus. You can access pop-up menu functions from the Selected menu.

Tree Views

You can expand or collapse a tree by pressing *Enter* or by using the left and right *arrow keys*. Pressing the **(*)** key does not expand a tree selection. Pressing the plus (+) and minus (-) keys on the numeric key pad does not expand or collapse the tree. Typing characters or pressing *Backspace* while on the tree does not select an item.

List Boxes

In a *list box*, press the *Down Arrow* and *Up Arrow* keys to select an item.

To select multiple sequential items Hold down the *Shift* key while pressing the Down or Up Arrow key.

To select multiple items that are not sequential:

- Hold down the *Ctrl* key
- Press the *Down* or *Up Arrow* key to move to the next item
- Release the *Ctrl* key
- Press the *Space bar*

To deselect the item:

- Hold down the *Ctrl* key
- Press the *Down* or *Up Arrow* key to move away from the item and then back to the item
- Release *Ctrl*
- Press the *Spacebar*

You cannot select items within a list box, list view, or tree by typing the characters of its name.

Within list boxes, the following actions have no effect:

- Pressing the *Ctrl* key with Page Up, Page Down, Home, or End
- Pressing a letter key
- Pressing *Shift+F8*

Radio Buttons

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

Notebook Tabs

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

Additional Keystrokes

The following keys have no effect on text fields:

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

Using Display Names

Certain windows, like the ones for defining attributes, item types, and MIME types, require a name and a display name. The Name field identifies an object to the system and represents the name used in the database for the object or attribute definition. The Name field once defined and stored cannot be modified. *The Display name field identifies the name that end users see when they work with the end user application. This field can be modified and also different strings can be defined on the attribute panel to represent different language translations*.

Note: Keep display names distinct from other display names. If you do not, you can confuse the end-user.

For example, you can have an attribute for someone's first name and use a display name of *Name*. You could also put *Name* as the display name of a person's last name. End users will see two attributes called *Name*, but they will not know which value to enter for each attribute.

You must define an attribute in every language that the attribute is used on your system, Figure 4–8 on page 134. If an attribute displays in a language that is different from the language defined on a machine, an asterisk (*****) displays before the attribute name.

Review Library Server Configuration Options

The *Library Server* stores, manages, and provides access control for content stored on one or more Resource Managers. The Library Server processes requests from one or more clients and maintains data integrity between all of the components in the Content Manager system. A single Library Server can support multiple Resource Managers and data can be stored on any of these Resource Managers. After you define a Library Server to the System Administration Client, you need to configure it.

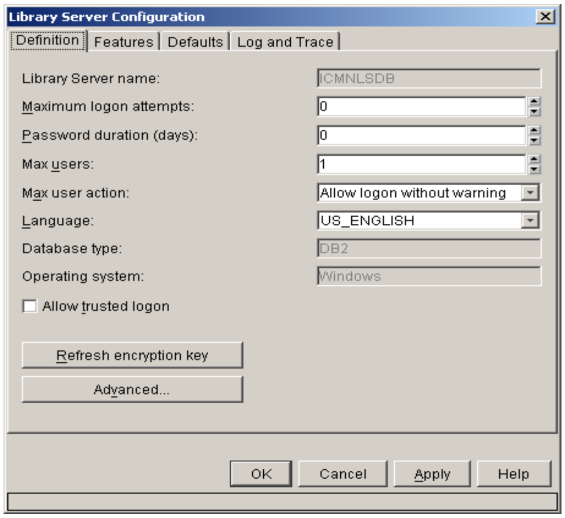
Library server configuration covers the following topics:

- Enabling trusted logons
- Refreshing the Encryption Keys to regenerate data base tokens
- System defaults for maximum users, logon attempts, and password duration
- What type of access users have to the system (default ACLs) and its objects (item level, item type level, mixed, or library level)
- Turning on and setting the system trace levels for troubleshooting errors
- Whether or not to log system administrator events
- Enabling Text Information Extender and setting the user ID and password

1. ___ Select **Library Server Parameters** and then **Configurations**.

2. ___ Now **open** the **Library Server Configuration**.

   This will display a dialog window with tabs named definition, features, defaults, log and trace. Many of the settings in this area will be stored in the Library Server database (*icmnlsdb*) table named - *ICMSTSYSCONTROL*. (Figure 4–6 shows an example of a Library Server configuration screen.)



Library Server name: ICMNLSDB

Maximum logon attempts: 0

Password duration (days): 0

Max users: 1

Max user action: Allow logon without warning

Language: US_ENGLISH

Database type: DB2

Operating system: Windows

☐ Allow trusted logon

Figure 4–6 *Library Server Configuration*

Definition Tab

On the Library Server Configuration *Definition* tab, do the following:

3. ___ **Set Maximum logon attempts to 5**, (the range can be from 1 to 32767).

4. ___ **Increase the Password duration to 200 days**, (the range can be from 1 to 32767).

> **Note:** Sets the system default password expiration timeframe to 200 days.

5. ___ **Set Max users to 5 concurrent users**, (the range can be from 1 to 32767).

Allowing Trusted Logon

When you set up your Library Server to allow trusted logon, you let users have access to the Library Server using their workstation password and without prompting for an additional password. You must complete the following procedure to allow for trusted logon:

6. ___ Notice that *Max user action* is set to **Allow logon without warning**.

> **Note:** This is required, along with *Allow trusted logon*, to enable single system sign-on.

7. ___ **Check** the *Allow trusted logon* box.

8.1

> **Note:** User IDs created for single logon will also need to have assigned the `ICMConnectToLogon` and `AllowTrustedLogon privileges` in their default privilege sets. If they are not assigned then the system asks for a password. Content Manager provides three default privilege sets with these privileges: AllPrivSet, System AdminPrivSet, and ICMTrustedLogonPrivSet.

Updating System Database Tokens

8. ___ Select **Refresh encryption key**.

8.1

> **Note:** This is where you refresh the encryption keys used by tokens throughout the Content Manager system for underlying data and object access. It is important that the Resource Manager be active and running when this is selected, otherwise the tokens for the Resource Manager will not be reset.

9. ___ Select **Yes**, on the warning/message window.

Set System Default ACL Binding

10. ___ Select the **Advanced** push button to set the Access Control List binding to one of the following values (see Table 4–2).

Table 4–2 *System Default Access Control List Binding*

Access Control List Default Binding	ICMSTSYSCONTROL Table ACLBINDINGLEVEL Column Value
Item Type	0
Item	1
Mixed (Item and Item Type)	2

Table 4–2 *System Default Access Control List Binding*

At the Library Level	3

If the *Public Access Enabled* box is unchecked, then all Access Control Lists that contain public access will be ignored. Likewise if it is checked then objects controlled by public access will be available to most users accessing the system. Select **cancel** to avoid making changes. Access control needs to be set at the item and item type for exercises that follow in this guide.

11. ___ Select **Apply**.

Features Tab

12. ___ Select the **Features** Tab.

13. ___ Notice that the *Enable Text Information Extender* has been selected.

The user ID *ICMADMIN* has already been set at installation. If you install Content Manager and then add DB2 Text Information Extender later, you will need to come to this panel to enable text search for the system.

14. ___ For now, retype the *password* as **password.**

When creating an item type and selecting text search options, if you encounter an error the first area to check is to make sure that the DB2 Text Information Extender has been started. Second, check this user ID and retype the password to make sure that it matches what is being used for the Text Information Extender.

15. ___ Select **apply**.

Defaults Tab

16. ___ Select the **Defaults** Tab.

17. ___ Notice that the *Default Access List* is set to **Item Type's ACL**.

This means that the system will use the access control list assigned to an *item type* as the default for access to stored objects. This could be set to the user's assigned access control list or the access control list assigned to the library. If it is assigned to the library, it is like granting public access because the underlying ACLs will be superseded by the access given to the library wide system.

18. ___ Leave the *Default Access List* set to **Item Type's ACL**.

19. ___ Notice also that Content Manager will allow the Resource Manager and collection to be determined by the user profile or the defined item type.

    This provides the capability to split out certain types of business objects represented by Item Types to specific *collections* and *volumes*. Or to have *assets* stored in Content Manager allocated to Resource Managers based on the user storing the asset.

20. ___ For purposes of this study guide, set the defaults for *Resource Manager* and *Collection* to **Item Type**.

Log and Trace Tab

In previous releases of Content Manager enabling *trace*, to troubleshoot problems with the Library Server, had to be set either in a start-up file or environment setting. The capability to turn on trace has been added to the Library Server Configuration area so that a System Administrator managing systems across platforms can initiate a Library Server trace in a consistent manner. *Due to the drain on the system resources, it is critical that tracing not be enabled other than for troubleshooting problems.* For more information about creating a trace log and the errors you get from your system, refer to the *Messages and Codes* (SC27-1349-00) manual.

21. ___ Select the **Log and Trace** tab**.**

22. ___ Select **Allow system administrator event logging**.

    This options allows the events corresponding to the actions taken while using the Content Manager System Administration program to be logged in the Library Server database table *ICMSTSYADMEVENT* table. After using some of the System Administration Client areas, bring up the DB2 Control Center and view (sample) the contents of this table to get an idea of the “audit trail” type of information that is logged.

23. ___ Use the Windows Explorer to locate the file **X:\Program Files\IBM\Cmgmt\ADMIN\COMMON\dklog.log**

    The location of this file may vary depending on the options taken when installing Content Manager. Errors encountered by the System Administration Client will be logged into the **x:\Program Files\IBM\Cmgmt\ADMIN\COMMON\dklog.log** file. Depending on the magnitude of the error, there may also be errors logged to the Library Server log file. The following is an extract from a *dklog* file showing an error for settings on the Item Type Text Search Options panel.

```
[EXC]: 08/07/2002 at 16:02:22.843 CDT @ edmbeta
(9.24.115.61); com.ibm.mm.sdk.common.DKException #
com.ibm.mm.sdk.logtool.DKLogManagerFactory_default

[USR]: cmadmin (C:\Documents and Settings\cmadmin) @
d:\Program Files\IBM\Cmgmt\admin\common

[THD]: AWT-EventQueue-0 ( 552c3d9f )

[THG]: main = { AWT-EventQueue-0,
SunToolkit.PostEventQueue-0, AWT-Windows,
AWT-InputMethodManager, TimerQueue, Thread-1, Screen Updater
}

[LOC]:
com.ibm.mm.sdk.server.PItemTypeDefImplCM:defineComponentType

[MSG]: DGL3894A: Error occurred while updating component
type; ICM7064: An unexpected error occurred when the
library server was requesting Text Information Extender
(TIE) to create, update, or delete a TIE index.  See the
library server log for more details.  Use the external
return code from library server to check the TIE error
message in DB2 UDB TIE documentation.  Correct the problem
and try again. (STATE) :

[LS RC = 7064, SQL RC = 107]
```

24. ___ Notice the *Trace level* area. At this point do not select a trace level.

The Library Server system *Trace* information by default is written to the *ICMSERVER.LOG*. The location and file can be changed on this panel. The default setting for the Trace filename is platform dependent (see Table 4–3).

Table 4–3 *Default Content Manager Library Server Log File*

Supported Platform	Default Server Logfile
Windows	C:\ICMSERVER.log
AIX, SUN	tmp/ICMSERVER.log

From a database perspective, Library Server tracing is controlled by two columns in the Library Server control table *ICMSTSYSCONTROL*: **Tracelevel** and **Tracefilename**. Table 4–4 on page 131 contains a listing of the corresponding database values for each of the available trace levels.

Table 4–4 *Content Manager Trace Levels Set in the Database*

Trace Level	Database Setting	Information Traced
No Trace	0	
Basic Trace	1	Entry and exit information to the Content Manager stored procedures and lower-level Library Server functions (for example, list NLS keywords).
Detailed	2	Basic trace information, plus information on the lower-level controls through the Library Server programming logic. This trace level provides information on how the program logic ran.
Data	4	Information on what input parameters were passed into the Content Manager stored procedures, and the intermediate data as the stored procedures were running.
Performance	8	Information on how fast the Content Manager stored procedures ran. The trace shows one line for each stored procedure and the elapsed time, in milliseconds, that the stored procedure took to run.
Basic and Detailed	3	Combined data from each of the above levels.
Basic and Data	5	Combined data from each of the above levels.
Basic and Performance	9	Combined data from each of the above levels.
All Options	15	Basic, Detailed, Data, Performance.
Database setting	16	Only build and parse, set using SQL.
Database setting	32	Memory management, set using SQL.
Database setting	63	All the GUI settings, build and parse, and memory management.

25. ___ Select **OK**

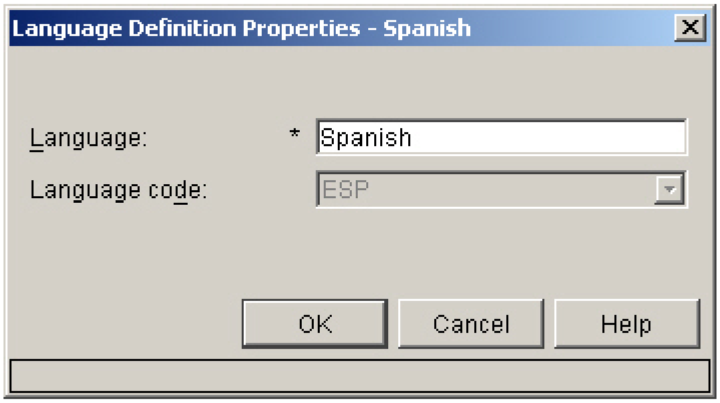
Exit the Library Server Configuration panel and **save** the changes.

Defining Language Codes

The Library Server by default is prepared to support multiple languages. You can have multiple languages enabled at the Library Server to support users running a specific Content Manager client version on their workstation. Or, users accessing the system through a dedicated Line of Business applications. When creating Data Model entities like attributes, item types, links, references, and others the System Administration Client allows translation strings to be added for the display names of the object. This is done by entering a translation string for the indicated Language code. Once done, a user querying the system will see the display names in the language being used with their clients. (See Table 4–5 on page 133 for an example of some of the language codes.)

1. ___ Select **Language Definitions**. Located under the Library Server Parameters.

2. ___ Create a new Language Definition (see Figure 4–7).



Language: * Spanish

Language code: ESP

Figure 4–7 *Screen for adding languages to Library Server*

3. ___ Type **Spanish** as the Language name.

4. ___ Select **ESP** as the language code.

Table 4–5 *Sample Language Codes*

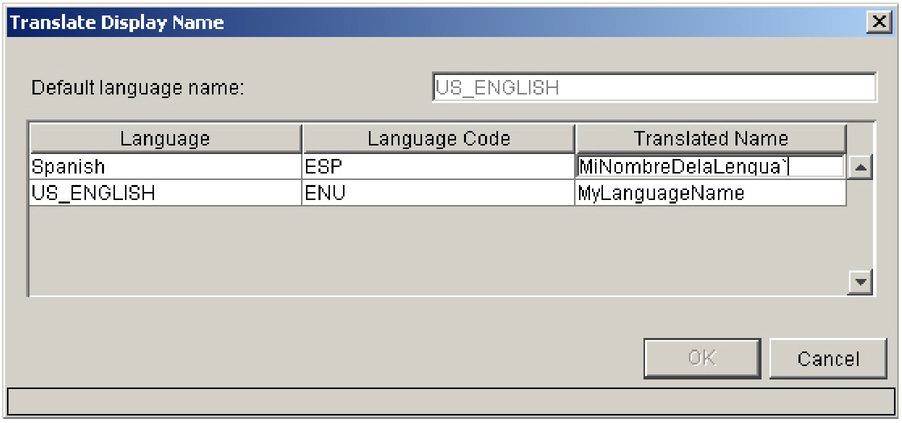
Language code	Language
ENG	English, United Kingdom
ENU	English, US
FRA	French
DEU	German
PTG	Portuguese
ESP	Spanish

Refer to the *System Administration Guide* (SC27-1335) for a complete list of language codes.

5. ___ Select **OK**.

Now lets experiment to see how adding the new language affects attributes added to the system.

6. ___ Select **Data Modeling** in the System Administration Client.
7. ___ Select **Attributes** and create a new Attribute.
8. ___ In the Name Field, type **MyLanguageName**. The same text should be entered in the Display name.
9. ___ Select the **Translate** button and the Translate Display Name panel opens (see Figure 4–8).



Default language name: US_ENGLISH

Language	Language Code	Translated Name
Spanish	ESP	MiNombreDelaLengua`
US_ENGLISH	ENU	MyLanguageName

Figure 4–8 *Content Manager Translate Display Name Panel*

10. ___ Type **MiNombreDelaLengua** as the text for the Spanish translation of *MyLanguageName*.

11. ___ Select **OK** to close the Translation screen and the Attribute Screen.

Resource Manager Configuration Parameters

The Resource Manager is the repository for the content and objects stored in the Content Manager system. When users save or import images, documents, photos, and other files into Content Manager, the attribute data associated with those images is stored in the Library Server tables and the object content is placed on the Resource Manager. Users perform queries against the Library Server, using the stored attributes, to locate an item (the stored entity). Once located the object or content associated with that item can be retrieved from the Resource Manager.

When a retrieve request is made, the Library Server returns a security token and the Resource Manager location for where the object is located to the client or calling application. The client uses the security token to access the indicated Resource Manager requesting the object for the referenced item. The object is transferred to the client or calling application using the enabled protocols for the Resource Manager

The default Resource Manager used when users or applications store objects is determined by either the user profile for that user or the defined Item Type for the object being stored. When a user is added to Content Manager they are assigned a default Resource Manager, collection, and access control list. Likewise, when parts are added to a document item type a default Resource Manager, collection, and access control list are assigned to the item type part. A Resource Manager can have multiple collections for separating different types of work. Items are stored using Collections which consist of a Storage Group and assigned Migration Policy.

The default Resource Manager and collection to be used is determine by the default settings in the Library Server Configuration. The default can be set to Item Type or User Profile.

Discussion on setting up the Resource Manager storage characteristics will be covered in the System Managed Storage section of this guide that describes integrating the IBM Tivoli Storage Manager.

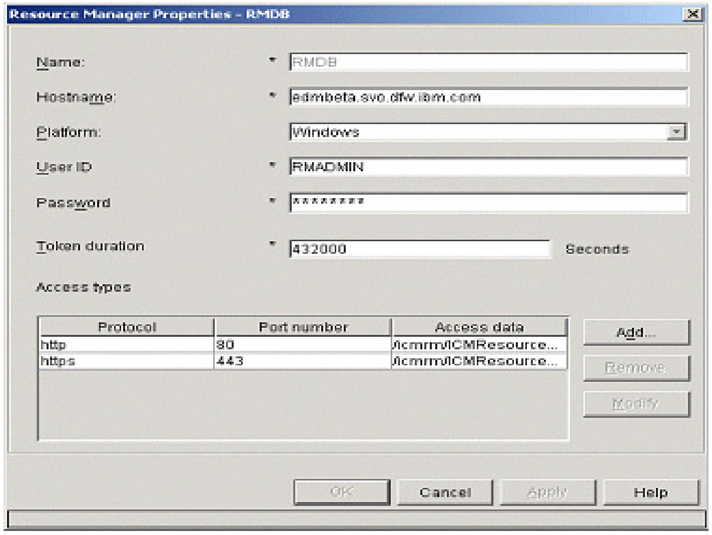
The remaining section here will cover the different Resource Manager parameters that can be adjusted: database connection, time outs, migration schedule and cycles, and protocols.

Note: The user ID and password of the Resource Manager that you want to access must match the user ID and password that you used to logon to the System Administration Client. If the user IDs and passwords are different, then you will get a prompt asking you for the user ID and password for that Resource Manager. You cannot configure or modify a Resource Manager unless you have access to it.

To configure your Resource Manager, go to the Resource Manager that you want to update. For example, use the following steps to review the configuration options of the Resource Manager added during the installation process.

Resource Manager Properties

1. ___ Expand the Resource Managers.
2. ___ Highlight the **RMDB** Resource Manager.
3. ___ Select the **Selected** menu bar item and then **Properties** to display Figure 4–9.



Resource Manager Properties - RMDB

Name: * RMDB

Hostname: * edmbeta.svo.dfw.ibm.com

Platform: Windows

User ID * RMADMIN

Password * ********

Token duration * 432000 Seconds

Access types

Protocol	Port number	Access data
http	80	/icmrm/ICMResource...
https	443	/icmrm/ICMResource...

Figure 4–9 *Resource Manager Properties*

4. ___ **Do not** make changes in the Resource Manager properties.

   Observe the required fields that were set when the Resource Manager was installed and deployed in the WebSphere Application Server.

   Hostname: A fully qualified hostname for where the Resource Manager resides. Use the fully qualified hostname for the Secured Socket Layer setup.

   User ID and Password: user ID and password used to access the Resource Manager database.

   Access Types: shows the ports used by the http and https protocols for accessing this instance of the Resource Manager. Make sure the https port is the one you setup as the Secured Socket Layer for the fully qualified hostname being used by the Resource Manager.

> 8.1
>
> **Note:** The Resource Manager is a web application and the property files for the Resource Manager are located by default at:
>
> **C:\WebSphere\AppServer\installedApps\icmrm.ear\icmrm.war\WEB-INF\classes\com\ibm\mm\icmrm\ ICMRM.properties**

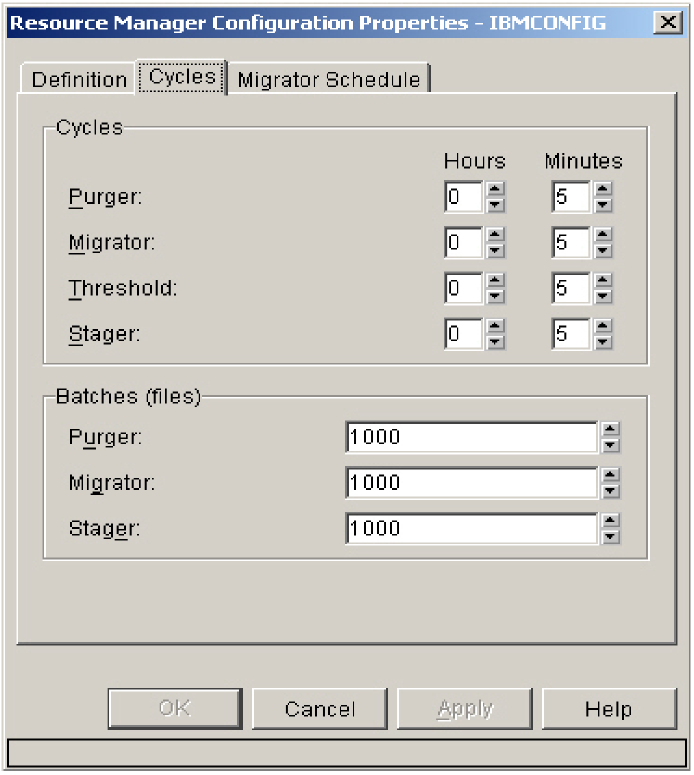
Resource Manager Configuration Properties

5. ___ Expand the Resource Managers.

6. ___ Select **Configurations**.

7. ___ Select **IBMCONFIG** to open the Resource Manager default configuration file (see Figure 4–10).

8. ___ Select the Definition, Cycles, and Migrator Schedule tabs to view options. Cycles is displayed in Figure 4–10.



Cycles

	Hours	Minutes
Purger:	0	5
Migrator:	0	5
Threshold:	0	5
Stager:	0	5

Batches (files)

Purger:	1000
Migrator:	1000
Stager:	1000

Figure 4–10 *Resource Manager Configuration Properties*

Timeout: Maximum amount of time the Resource Manager should wait for a response from the library server, clients, or purger process.

Cycles: The amount of time that must elapse before the Purger, Migrator, Threshold, and Stager kickoff.

Batches: The number of files or objects in a process batch for the purger, migrator, or stager.

Migration Schedule: Time spans for setting the time frames for when objects will be migrated.

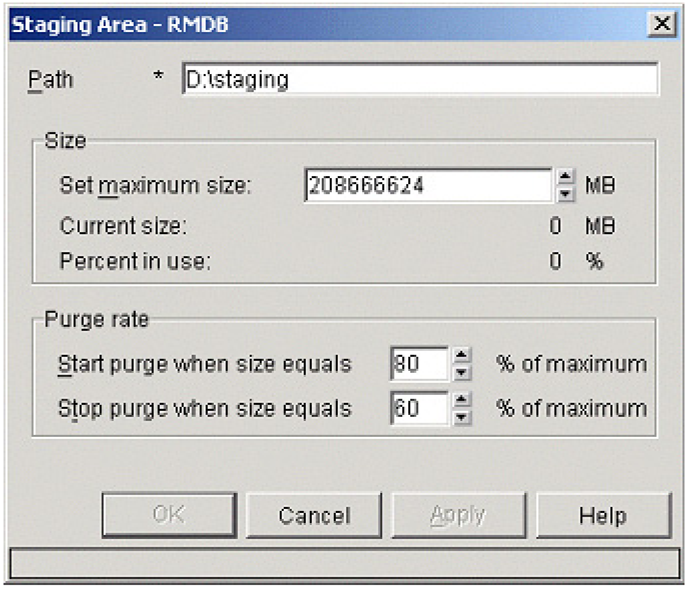
9. ___ Select **Cancel** to exit.

Resource Manager Staging Properties

10. ___ Expand the **Resource Managers**.

11. ___ Highlight the **RMDB** Resource Manager.

12. ___ Select the **Staging Area,** Figure 4–11.



Staging Area - RMDB

Path * D:\staging

Size

Set maximum size: 208666624 MB

Current size: 0 MB

Percent in use: 0 %

Purge rate

Start purge when size equals 80 % of maximum

Stop purge when size equals 60 % of maximum

Figure 4–11 *Resource Manager staging settings*

This screen shows the path of the staging file, the maximum size and purging parameters.

Note: In previous Content Manager releases, the staging area was used for transferring files between the clients and object server. In Version 8 it is used for transferring files from SMS volumes managed by Tivoli Storage Manager.

13. ___ Select **Cancel** to exit the Resource Manager properties.

You will work with the other objects under the Resource Manager later on in the Study Guide lab exercises.

Other Server Configuration Options

This section will review other configuration options that affect the overall system.

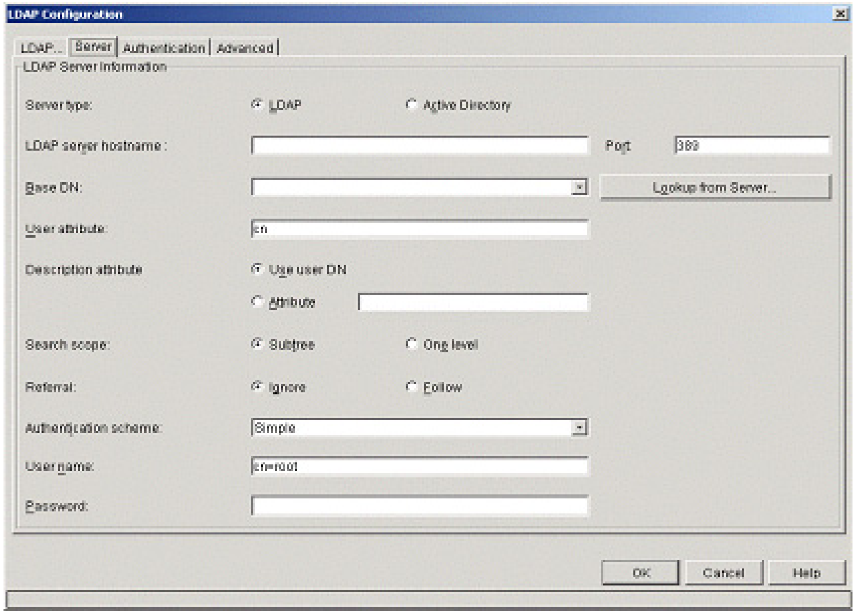
LDAP Server Configuration Options

1. ___ Select the **Tools menu** bar item and then **LDAP** Configuration.

The LDAP Configuration screen is presented so that you can enable importing data sources from an LDAP server. The other tabs are not selectable because LDAP has not been setup.

2. Select **Enable importing of Datasources from LDAP** in order to view the other tabs under the LDAP Configuration area.

3. ___ Select the LDAP **Server** tab Figure 4–12.



LDAP Server Information

Server type: ● LDAP ○ Active Directory

LDAP server hostname:

Port 389

Base DN:

User attribute: cn

Description attribute ● Use user DN ○ Attribute

Search scope: ● Subtree ○ One level

Referral: ● Ignore ○ Follow

Authentication scheme: Simple

User name: cn=root

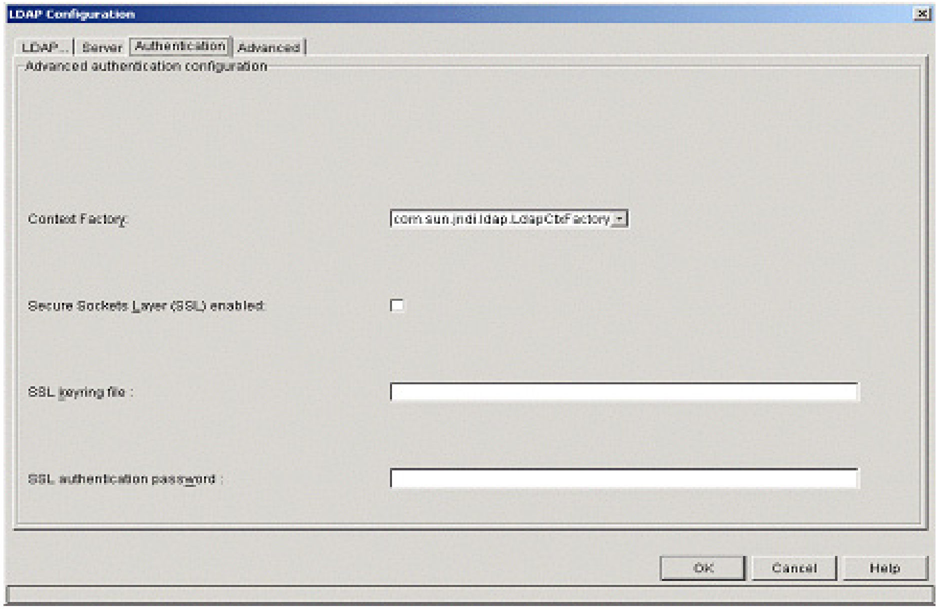
Password:

Figure 4–12 *LDAP Server Configuration Information*

4. ___ **Observe** the LDAP Server settings that would have to be configured if LDAP was enabled at this point.

Note: LDAP will be setup later in this study guide. Notice that in order to import LDAP data, both the BASE Domain Name and User Attribute field will have to be declared on this screen.

5. ___ Select the LDAP **Authentication** tab (see Figure 4–13).



Context Factory: com.sun.jndi.ldap.LdapCtxFactory

Secure Sockets Layer (SSL) enabled: ☐

SSL keyring file :

SSL authentication password :

Figure 4–13 *LDAP Server Configuration Authentication*

6. ___ **Observe** the LDAP Authentication settings where the Secured Socket Layer access can be set for LDAP connection.

7. ___ Select the **Advanced** tab.

This is used to set the maximum number of records to retrieve from LDAP and the server connection timeout value.

8. ___ Select **Cancel** to exit the LDAP Configuration screen.

Users Logged on to the System

1. ___ Select the **Tools** menu bar item.

2. ___ Select **List Users**.

   This will show the number of users currently on the system.

3. ___ Select **cancel** to close the dialog.

This is the end of the System Administration Client and Server Configuration sections. You can close the System Administration Client.

Summary

Before installing Content Manager, it is important that time be spent determining the configuration of the Content Manager servers. Many of the Library Server and Resource Manager settings are determined from the information entered during the installation process. Once the product has been installed, the Library Server and Resource Manager configuration areas will allow many of the configuration options to be modified.

This chapter covered the general configuration topics to provide an overview of the System Administration Client and Content Manager servers, as well as areas that may be represented on the certification exam.

CHAPTER 5

Managing System Access

- Administrative Domains
- Users and Groups
- Privilege Sets
- Access Control Lists

*M*anaging access to the Content Manager system involves creating Content Manager based user IDs and assigning those user IDs privileges. The user assigned privileges define the maximum operation a user can perform in accessing areas of the Content Manager system and for accessing content stored in Content Manager. Along with the user granted rights, content stored in Content Manager is also given a set of privileges contained in what is called an Access Control List (ACL). The ACL defines the maximum privileges or actions that can be performed against a stored object or within a document routing process. When accessing an object that grants greater privileges through its associated ACL, a user's effective access rights will not exceed the user's defined privileges granted in their user profile, unless the user is specifically listed in the ACL and granted specific rights. Along with covering users, privileges, and access control lists, this section will cover administrative domains, a new feature added in Content Manager. Administrative domains allow the system administrator to divide users into different domains granting domain administrative rights to a user solely responsible for the domain.

Administrative Domains

Administrative domains have been added to Content Manager so that the administrative tasks of managing users and access to stored objects can be relegated to more than a single system administrator (see Figure 5–1). Domains allow a single Content Manager system to be used in support of multiple departments or business areas where an administrator from those areas has responsibility to manage the users accessing their domain. Essentially, all users in each area are using a single Content Manager Library Server and their associated Resource Managers, but with restricted access to the overall system. It is important to understand the following restrictions prior to enabling administrative domains:

- Once enabled, administrative domains cannot be disabled.
- The three default domains cannot be modified.
- The administrative objects from the default domains cannot be deleted.
- ICMPublic user group cannot moved outside the default public domain.
- Common across Content Manager and EIP if sharing the same database.

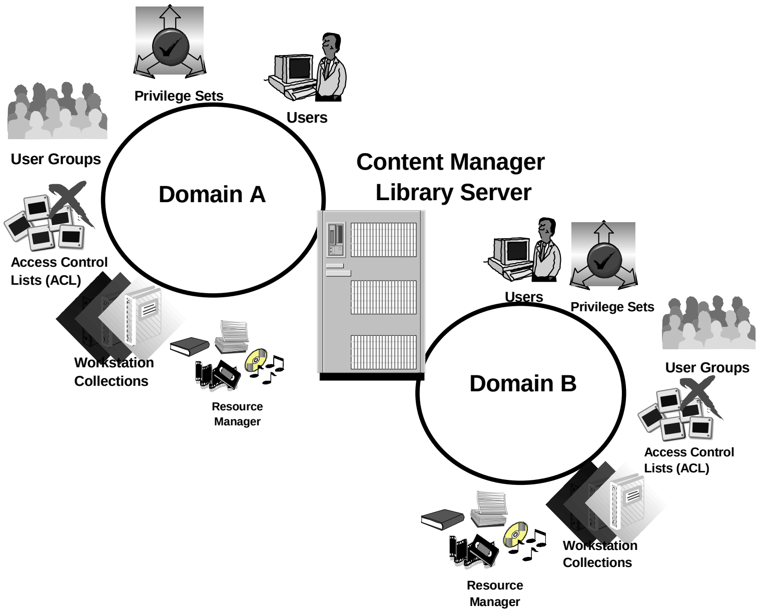


Figure 5–1 *Resources effected by Administrative Domains*

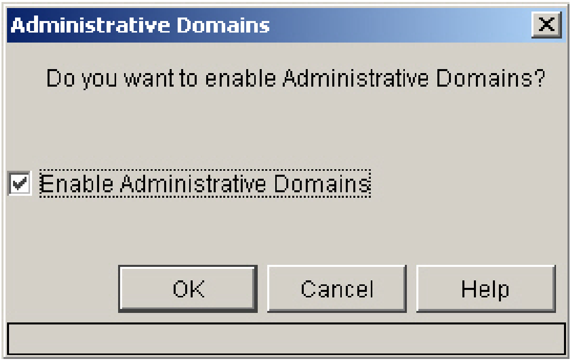
Each of the following items can be assigned to an administrative domain that would preclude users in other domains from accessing the assigned items:

- Resource Manager
- Workstation Collection
- Users and User Groups
- Privilege Set *(can be assigned to multiple domains)*
- Access Control List *(can be assigned to multiple domains)*

Because domains are meant to limit access to areas of the system, an administrator with super access like the *ICMADMIN* user ID can setup the domains and define an administrator for the domain. This is done by creating a user, assigning the user to the domain, and then assigning the correct privilege set (for example, *SysAdminSubDomainCM*) to the user profile. It is **important** that the user profile also be given the correct privilege set for *Grant privilege set*. This limits the domain administrator's authority for granting privileges to other users beyond the authority of the administrator. This sub-domain administrator would be restricted to creating users within their domain, allocating privilege sets and access control based on what has been assigned to the domain by the overall system administrator.

Enable Administrative Domains

1. ___ Start the **System Administration Client**.
2. ___ Select **Tools**.
3. ___ Select **Administrative Domains** to display the enablement screen (see Figure 5–2 on page 148).



Do you want to enable Administrative Domains?

☑ Enable Administrative Domains

Figure 5–2 *Administrative Domains Enablement Screen*

4. ___ Select **Enable Administrative Domains**.

5. ___ Select **OK**.

You will be presented a warning screen with the following message. It is critical you realize that administrative domains cannot be turned off once initiated.

> **Warning!!!!** Once Administrative Domains is enabled, it CANNOT be disabled. Refer to sections on Administrative Domains in the System Administration Guide.

6. ___ Select **Yes** to complete the enablement.

7. ___ Select **OK** on the *Administrative Domains is now Enabled* screen.

8. ___ **Close** the System Administration Client**.**

9. ___ **Restart** the System Administration Client.

You should see Administrative Domains, with three default domains, added to the list of administrative areas for Content Manager (see Figure 5–3 on page 149).

.

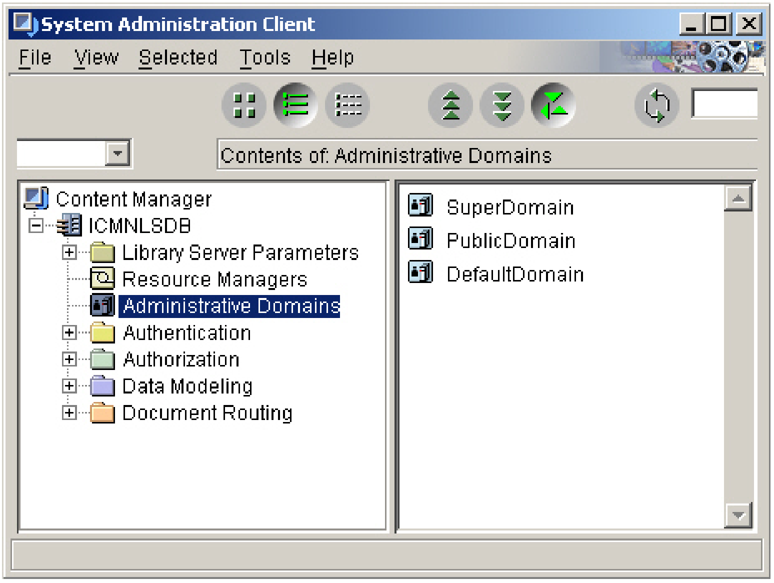


Figure 5–3 *System Administration Client with Administrative Domains*

Table 5–1 describes the default domains.

Table 5–1 *Default Administrative Domains*

Default Domains	**Purpose**
SuperDomain	Used for super system administration access to all Content Manager services. The ICMADMIN user ID belongs to this domain by default and cannot be moved. In addition, all default privilege sets and Access Control Lists belong to this domain so an administrator with super system access can control all parts of the Content Manager system.
PublicDomain	Default used for public access to parts of the system. The ICMPublic user group belongs to this default domain and cannot be moved. In addition, this domain can be assigned to groups to insure that members in the group maintain the domain access defined in their individual user profiles.

Table 5–1 *Default Administrative Domains*

Default Domains	Purpose
DefaultDomain	Default domain designed to accommodate sub-administration or administrators responsible for a particular domain. When creating new users, this would be the default domain most used unless specific domains are created.

Add Administrative Domains

To accommodate activities in later sections of this manual, two administrative domains will be setup.

10. ___ Highlight **Administrative Domains** and Select **New**.

11. ___ Type **PhotoLab** as the domain name.

12. ___ Type **Photo processing group** as the description.

13. ___ Select **OK**.

14. ___ Highlight **Administrative Domains** and Select **New**.

15. ___ Type **AdvertisingMedia** as the domain name.

16. ___ Type **Multimedia advertisement department** as the description.

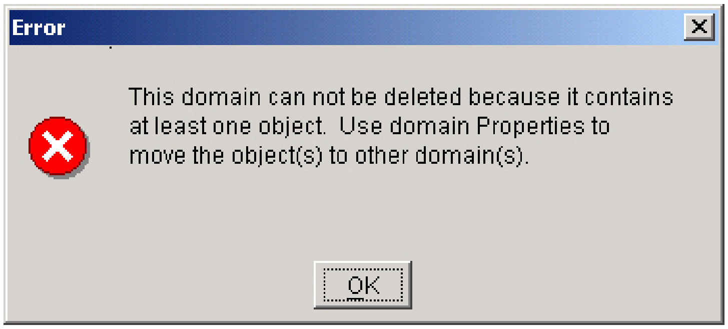
17. ___ Select **OK**.

Note: The domain name is a label. The definition of the domain is the privileges, access control lists, users, collections, and Resource Managers assigned to the domain.

You should see both domains listed with the default administrative domains. Once the domains are created, the next set of actions is to create and assign to the domain users and groups, privilege sets, and access control lists. In addition, a dedicated Resource Manager and workstation collection can be assigned to the domain.

Note: Once users, privilege sets, access controls, and other objects are assigned to the domain, the domain cannot be deleted until all objects are re-assigned to another domain.

It is **important** to remember that once objects like users and access control lists have been added to a domain, the domain cannot be deleted. If you desire to remove the user defined domain, you must first reassign all users, user groups, Resource Managers, and workstation collections to other domains. In addition, assuming you have added privilege sets and access control lists to the domain and shared them with other domains, then they must be removed from the domain to be deleted. If any objects remain in the domain, then the error shown in Figure 5–4 will be displayed when an attempt is made to remove the domain.



This domain can not be deleted because it contains at least one object. Use domain Properties to move the object(s) to other domain(s).

Figure 5–4 *Error message when attempting to delete a domain*

The following sections will highlight how each area is effected by administrative domains. Completely setting up administrative domains and discussing all the affects on the system is beyond this study guide. Refer to the Content Manager for Multiplatforms System Administration Guide for more information.

Create Privileges and Privilege sets

The first task in defining the access control for your system is to create any additional privileges that are needed and then define privilege sets that can be assigned to users and used in access control lists. If administrative domains are being used, then the privilege sets need to be added to the domain for which they apply. Privileges grant rights to allow a user to perform a specific action on an item or object in the system such as create, delete or select. Content Manager provides a number of predefined privileges that you cannot change. You can define your own user defined privileges. Table 5–2 lists the predefined privileges shipped with Content Manager and the areas they cover.

Table 5–2 *Predefined privileges installed with Content Manager*

Predefined Privileges	Area Privileges Cover
AllowConnectToLogon AllowTrustedLogon	Privileges affecting how users can logon.
Privileges starting with *Client* like ClientScan and ClientImport	System defined privileges starting with *Client* apply to enabling different capabilities a user can perform using the Content Manager clients.
Privileges starting with *EIP*	Applies to administrating the objects that can be created in the EIP defined database. Only applicable if EIP has been installed with Content Manager.
Privileges starting with *IKF*	Controls actions for the EIP Information Mining facility. Only applicable if EIP has been installed with Content Manager.
Privileges starting with *Item*	Privileges that govern actions performed on items. This includes actions on items, document parts, and objects.
Privileges starting with *System*	Predominately applies to actions administrators can perform on the system such as defining items, domains, attributes, access control lists, and other system actions.
Privileges starting with *WF*	Applies to the capability to affect EIP workflows and worklists.

You can use the *system* privileges to model user data and to administer and maintain the Content Manager system. You need system administration privileges to complete tasks such as configuring the system, managing the

Library Server configuration, and managing item types. You can use the *Item* privileges to access and modify the system data, such as items and item types.

Create Privileges

1. ___ Logon to the System Administration Client with **ICMADMIN** and **password**.
2. ___ Expand **Authorization**.
3. ___ Highlight **Privileges**. Create a new privilege.
4. ___ Type **MyPrivilege** for the privilege name.
5. ___ Type **My defined privilege** in the description field.
6. ___ Select **OK**.

   You should see *MyPrivilege* added to the list of privileges.

Create Privilege Groups

A convenient way of handling privileges is to group them into Privilege Groups containing the necessary system-defined and user-defined privileges. This makes assigning privileges to privilege sets much easier.

Note: Understand, it is the privilege set, with the assigned individual privileges, that are used for granting rights or privileges to users and access control lists.

1. ___ Highlight **Privilege Group**. Create a new privilege group.
2. ___ Type **MyPrivilegeGroup** for the name.
3. ___ Type **My created privilege group** for the description.
4. ___ Add all the privileges **except** the ones that start with *System*, *IKF*, *WF*, and *EIP*. This should move the privileges that start with: *Allow*, *Item*, *Client*, and *MyPrivilege* to the selected privileges area.

8.1

Note: Two important privileges that must be assigned to a Privilege Set for single user a sign-on are: **AllowConnectToLogon** and **AllowTrustedLogon**.

5. ___ Select **OK**.

You should see the *MyPrivilegeGroup* added to the list of privilege groups. The above steps to create privileges and privilege groups were taken so you would have a familiarity with how both are added to the system. For the sake of the remaining exercises in this guide, the predefined privileges and groups will be used.

Create Privilege Sets

A *privilege set* is a group of selected privileges brought together to grant rights to perform various actions within the Content Manager system. The assigned privileges can be from any of the defined groups. Groups are a convenience for organizing privileges around the different user roles or tasks for assigning to privilege sets. A privilege set can represent roles for different users accessing the system. The default privilege sets shipped with Content Manager (Table 5–3 on page 155) are organized around roles. These predefined privilege sets cannot be modified to add or remove privileges. The predefined privilege sets can be used as a base for new privilege sets by copying the privilege set.

Privilege sets are assigned directly to user profiles to grant user rights for performing tasks within Content Manager. The assigned privilege set contains the maximum rights the user has within the system. Privilege sets are also used to assign users and groups privileges within an access control list. When the access control list is assigned to an item, it defines the users and groups who have access to that item and the maximum rights for the user or group.

In this section, you will use the predefined privilege groups to create a privilege set.

Table 5–3 *Content Manager predefined privilege sets*

Privilege Set	Actions and tasks covered by the privilege set.
AllPrivs	Allow system administrator to have all privileges, including all client privileges.
NoPrivs	Assigns no privileges to a user. Use this privilege set for a temporary user setting.
ClientUserAllPrivs	Allow user to search documents, perform process and folder related actions such as start and stop for document routing, import items, change attribute values, and update notes and annotations.
ClientUserCreateAndDelete	Load documents into Content Management, including the ability to import and scan items, index documents, start items on workflow, and delete an item.
ClientUserEdit	Update items, annotations, note logs and perform searches, view document and print documents. This user can also perform folder actions and process related actions such as start and stop for document routing.
ClientUserReadOnly	Allow to perform read only tasks including search, view documents, annotations and note logs, and print documents. Excludes the ability to perform process-related actions, folder-related actions or make any updates.
SysAdminCM	Allow system administrator to manage users, groups, privileges, access control lists and administer the data model, servers, administrative domains. This administrator also has all client user privileges.
SysAdminSubDomainCM	Allow system administrator to work with the following objects in sub-domains: users, groups, privilege sets, access control lists, collections, and Resource Manager. This administrator also has all client user privileges.
SysAdminSuper	Allow system administrator to perform all system administration tasks for both Content Manager and EIP, including working with administrative domains. This administrator also has all client user privileges.
UserDB2Connect	Allows Content Management users to connect to DB2 without having their own DB2 user ID. This user is required to enter a password.

Table 5–3 *Content Manager predefined privilege sets*

Privilege Set	Actions and tasks covered by the privilege set.
UserDB2TrustedConnect	Allows Content Management users to connect to DB2 without having their own DB2 user ID. This user is not required to enter a password.

1. ___ Highlight **Privilege Sets.**

   You must group privileges into a set before you can use or assign them to users and access control lists. There is no limitation on the number of privileges a set can contain. Spend a few minutes reviewing the predefined privilege sets. The first set you create will be from an existing privilege set.

2. ___ Highlight the privilege set named: ***ClientUserCreateAndDelete***

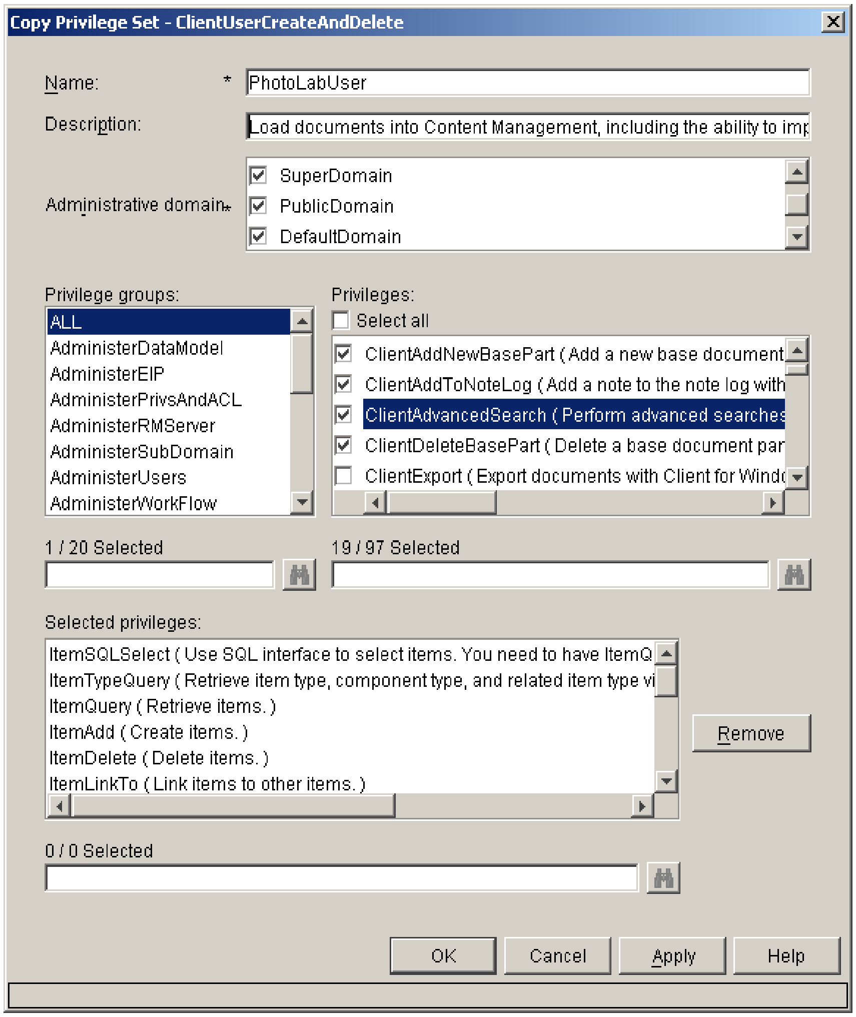
3. ___ Use the *Selected* menu to select **copy**. This will display the privilege set window allowing one to copy the privilege set.

4. ___ Type **PhotoLabUser** as the name**.**

8.1

> **Note:** On the *Copy Privilege Set* screen, (see Figure 5–5) notice the Administrative domain field. This is used to assign the privilege set to one or more domains.

5. ___ Notice that the three default administrative domains have been selected. Select the **PhotoLab** and **AdvertisingMedia** domains so the privilege set applies to all defined domains.



Copy Privilege Set - ClientUserCreateAndDelete

Name: * PhotoLabUser

Description: Load documents into Content Management, including the ability to imp

Administrative domain: ☑ SuperDomain ☑ PublicDomain ☑ DefaultDomain

Privilege groups:
ALL
AdministerDataModel
AdministerEIP
AdministerPrivsAndACL
AdministerRMServer
AdministerSubDomain
AdministerUsers
AdministerWorkFlow

1 / 20 Selected

Privileges:
□ Select all
☑ ClientAddNewBasePart (Add a new base document
☑ ClientAddToNoteLog (Add a note to the note log with
☑ ClientAdvancedSearch (Perform advanced searches
☑ ClientDeleteBasePart (Delete a base document par
□ ClientExport (Export documents with Client for Windo

19 / 97 Selected

Selected privileges:
ItemSQLSelect (Use SQL interface to select items. You need to have ItemQ
ItemTypeQuery (Retrieve item type, component type, and related item type vi
ItemQuery (Retrieve items.)
ItemAdd (Create items.)
ItemDelete (Delete items.)
ItemLinkTo (Link items to other items.)

0 / 0 Selected

Figure 5–5 *Privilege Set copied from a predefined system privilege set*

6. ___ Notice under **Privileges** that a number of the client privileges have not been selected. Select the following:

- ClientAddToNoteLog
- ClientAdvancedSearch
- ClientPrint
- MyPrivilege.

7. ___ Select **OK**.

   Now create a specific administrative privilege set.

8. ___ Highlight **Privilege Sets.** Create a new privilege set.
9. ___ Type **PhotoLabAdmin** for the name.
10. ___ Type **Administrate the Photo Lab** for the description. You can provide a description if desired.
11. ___ Select the **PhotoLab** and **AdvertisingMedia** domains.
12. ___ Under **Privilege groups** highlight the indicated privilege group and select the privileges indicated in Table 5–4.

Table 5–4 *Privileges to be assigned to the privilege set*

Privilege Group	Selected Privileges
AdministerSubDomain	SystemDomainAdmin SystemDomainQuery
AdministerUsers	SystemGrantUserPrivs SystemQueryGroup SystemQueryUserPrivs
MyPrivilegeGroup	AllowConnectToLogon AllowTrustedLogon

13. ___ Select **OK** to save the privilege set.

You should see **PhotoLabAdmin** added to the list of privilege sets. The following are Library Server tables that contain information for defined privileges (see Table 5–5).

Table 5–5 *Library tables holding privilege information*

Table	Purpose
Privilege Definition Table (ICMSTPrivDefs)	Maintains the unlimited number of CM privilege definitions, including both CM System-defined and User-defined. When defining or updating Privilege Sets, this table can be first queried to list all defined privileges. Privilege name and description are defined in the NLS Keywords Table (ICMSTNLSKEYWORDS).

Table 5–5 *Library tables holding privilege information*

Table	Purpose
Privilege Set Code Table (ICMSTPrivSetCodes)	Maintains the Privilege Set definitions uniquely identified by a CM system-generated code. Set-member associations are stored in the table ICMSTPrivSets.
Privilege Set Table (ICMSTPrivSets)	Maintains associations of CM Privileges with the Privilege Sets. Rows with the same PrivSetCode form a Privilege Set. Rows in this table can only be deleted, not updated.
Domain Privilege Set Table (ICMSTDomainPrivSet	Maintains associations of CM Privilege sets with the domain. Rows with the same DomainID form a domain’s privilege set. Rows in this table can only be deleted, not updated.
Privilege Group Code Table (ICMSTPrivGroupCode)	Maintains associations of CM Privilege sets with the domain. Rows with the same DomainID form a domain’s privilege set. Rows in this table can only be deleted, not updated.
Privilege Group Table (ICMSTPrivGroups)	Maintains associations of CM Privileges with the Privilege Groups. Rows with the same PrivGroupCode form a Privilege Group. Rows in this table can only be deleted, not updated.

Creating Users and User Groups

Before moving on to access control lists, you need to create some users. When creating the access control list, one must match a user or groups to a privilege set. In this section, you will create users to match the domains and privileges setup above. The exception will be for the Resource Manager and Collections, where the defaults created on install are assigned to the public or default domain. If you are managing domains and want users to only work from a specific workstation collection and Resource Manager assigned for the domain, these would be selected in the users profile. Setting up collections will be covered later in this guide when the Resource Manager System Managed Storage facilities are covered (see Figure 5–6).

Content Manager users are assigned privileges through associated privilege sets when their user profile is created. The user can belong to one or a number of groups as a means to conveniently organize users. Essentially, the user is a member of the group. Associating users with a group simplifies the process for creating access control lists. When defining access control lists, a group can be granted a number of privileges for all users at the same time instead of directly assigning the same privilege to each individual user in the group. It is important to realize that privileges reside with the user and the object for which the access control list controls. Groups are not directly assigned privilege sets. Also, a group cannot belong to other groups.

1. ___ Expand **Authentication**.
2. ___ Highlight **User Groups**. Create a New Group.
3. ___ Type **PhotoLabUsers**. You can provide a description if desired.
4. ___ Select **DefaultDomain** for Administrative Domain (see Figure 5–7 on page 163).
5. ___ Select the **New User** push button on the **New User Group** dialog.
6. ___ On the New User dialogue, type **PhotoTech** as the User Name.
7. ___ For Administrative Domain, select **DefaultDomain** (see Figure 5–6).

   Because you will not cover setting up a second Resource Manager with its own collections, create the users for the photolab using the DefaultDomain. Our purpose in this guide is to point out how Administrative Domains affect the user authorization and authentication areas. Setting up multiple domains and managing resources between those domains is beyond the scope of this certification study guide.

8. ___ Set the **Password** to password.

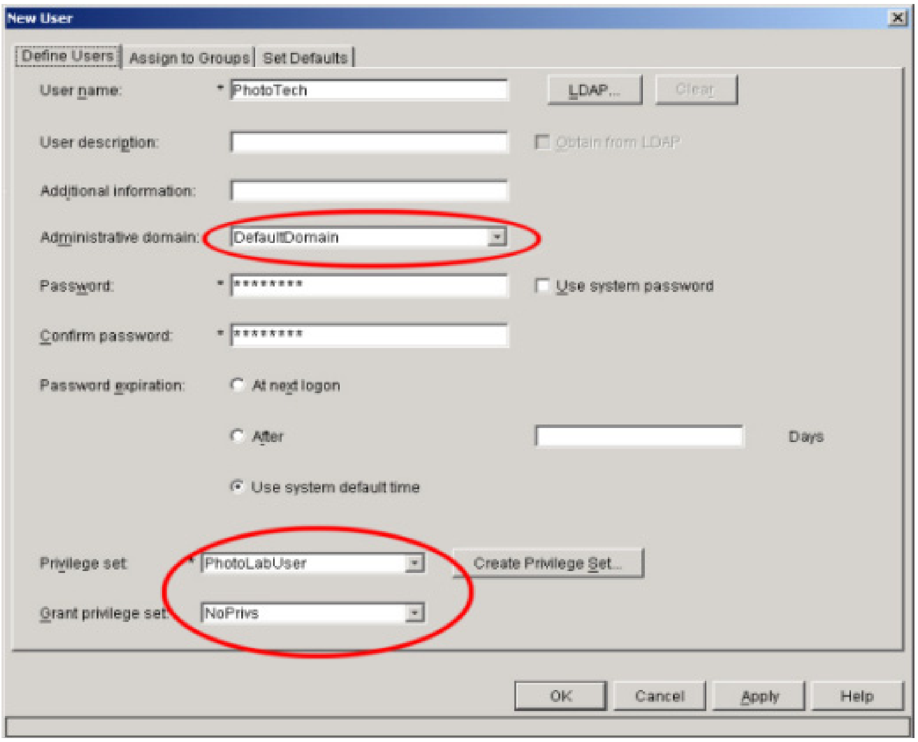
9. ___ Set the password expiration to **Use system default time**.

10. ___ Set **Privilege set** to **PhotoLabUser**.

Even though you are not using the PhotoLab domain, you can use this privilege set because you assigned the privilege set to each of the existing default domains.

11. ___ Set **Grant privilege set** to **NoPrivs**.

Note: Maximum level of privileges that this user can grant to other users when they have the authority to create users. In this case no privileges can be granted.



New User

Define Users | Assign to Groups | Set Defaults

User name: * PhotoTech

User description:

Additional information:

Administrative domain: DefaultDomain

Password: * ********

☐ Use system password

Confirm password: * ********

Password expiration: ○ At next logon

○ After ___ Days

● Use system default time

Privilege set: * PhotoLabUser

Grant privilege set: NoPrivs

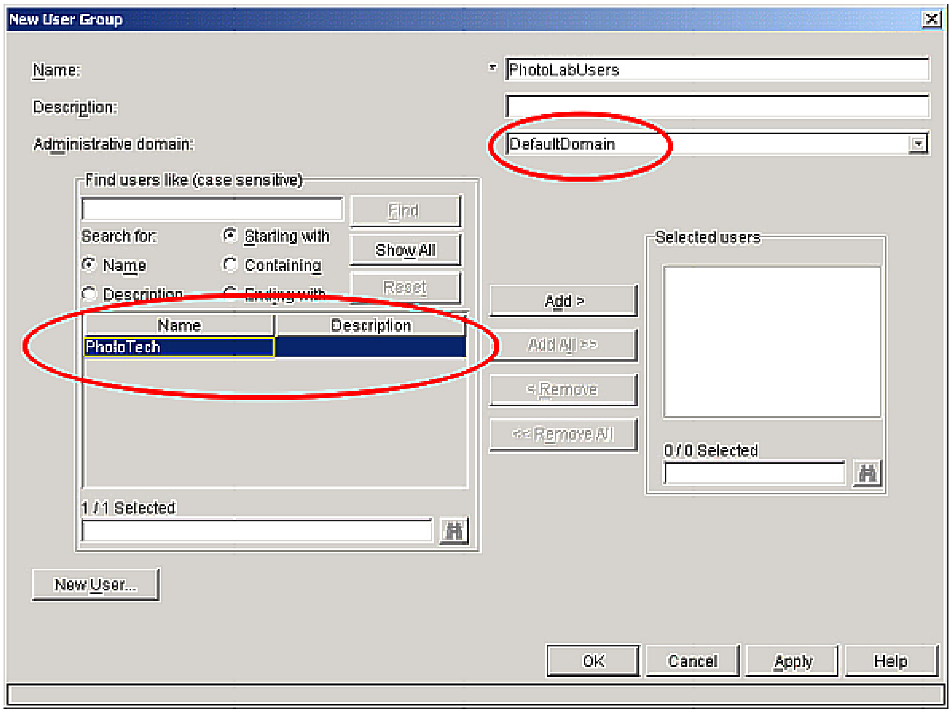
Figure 5–6 *New User Screen Showing Administrative Domain and Grant Privileges.*

12. ___ Select **Set Defaults tab**

For the user you need to specify the default Resource Manager, workstation collection (contains the target storage group and migration policy), and access control list. When managing a domain, you can have users using the default collection or a specific collection for the domain. If you want to divide or separate the data and content stored by the domain, then at a minimum you will need a workstation collection for each domain. You can have multiple workstation collections for a Resource Manager. With the Resource Manager assigned to the public or default domain, users from the different domains using their workstation collections can store and retrieve items from the Resource Manager. In some cases, you may want different domains to have their own Resource Manager if users in the different domains do not need to share content.

13. ___ Select **RMDB** for the default Resource Manager.
14. ___ Select **CBR.CLLCT001** as the default collection.
15. ___ Take the default shown on the default access control list.
16. ___ Select **OK.**

This returns you to the New User Group panel.


New User Group

Name: PhotoLabUsers

Description:

Administrative domain: DefaultDomain

Find users like (case sensitive)

Search for: ● Name ○ Description

● Starting with ○ Containing ○ Ending with

Name	Description
PhotoTech	

1 / 1 Selected

Selected users

0 / 0 Selected

Figure 5–7 *New User Group Screen With Added User.*

17. ___ Highlight the *user name* that was added.

18. ___ Select **Add** to move the user into the selected area.

Now create a second user for the domain administrator.

19. ___ Select the **New User** push button on the New User Group dialog.

20. ___ On the New User dialog, type **PhotoLabAdmin** as the User Name.

21. ___ Set the **password** to password.

22. ___ Set the password expiration to **Use system default time**.

23. ___ Set **Privilege set** to **PhotoLabAdmin**.

24. ___ Set **Grant privilege set** to **PhotoLabAdmin**.

8.1

> **Note:** PhotoLabAdmin admnistrative user ID will be able to create a new user and grant that user privileges up to and including the domain administrative privileges in PhotoLabAdmin.

25. ___ Select **OK**, to save the user.

26. ___ Highlight the user name that was added.

27. ___ Select **Add** to move the user into the selected area.

28. ___ Select **OK** to save the user group.

Alternatively, you could have made a separate group for our PhotoLab administrators in order to assign different privileges to each group. In an operational system, you would want to separate these roles so that users were not mistakenly granted privileges intended for administrators through access control lists. It is important to note that the group itself cannot belong to another group and the group acts as a convenient way to organize users and of itself does not contain default privileges for the users. As you added the group, you did not see a place on the group screen for assigning privileges. This is because privileges go with the user and object that is being stored into the system. If you look at the two user profiles you just created and select the group folder tab, you will see the new group has been assigned to each user.

Before moving on, review the following tables (see Table 5–6) that apply to the user and group definitions.

Table 5–6 *User and User Groups Library Server Tables*

Table Name	Purpose
User Table (ICMSTUsers)	This table maintains a catalog of individual users and user groups. Users are assigned a number of privileges, stored in UserPrivSetCode table. A group cannot belong to other groups. A group does not hold default privileges for its members.
User Group Table (ICMSTUserGroups)	This table maintains associations of individual users with user groups. The individual user and the group must be defined in the ICMSTUsers table before an association can be made between the user and the group.

Assigning Access Control Lists

Content Manager *access control lists* (ACLs) are essentially an association between a list of users and a list of granted privileges. To create an access control list, users or user groups are selected and associated to a privilege set. A single ACL can have multiple user/user group(s) and privilege set associations. The benefit of this approach is that a single ACL can be assigned to objects stored in the system and if there is a need to modify the privileges controlling the object it can be done in the ACL.

ACLs are used to control user access to objects stored in the system. Whereas, privilege sets assigned directly to the user profile define the maximum privileges the user has within the Content Manager system, ACLs are used to further restrict the user's assigned privileges for a particular object or item. ACLs cannot grant the user greater privileges than what they already have in their user profile assigned privilege set. The following are the Content Manager objects that are controlled by access control lists or for which an access control list can be assigned:

- Restrict public access to the library system
- Item Type *(definition for stored objects)*
- Item Type Subset
- Item *(an entity like a folder)*
- Part or stored object
- Document routing work node
- Document routing process
- Document routing worklists

The default behavior or precedence for how access control lists behave within the Content Manager system is set on the *Advanced Library Server Configuration* screen. Default access or access control list binding can be set to one of the following for the system:

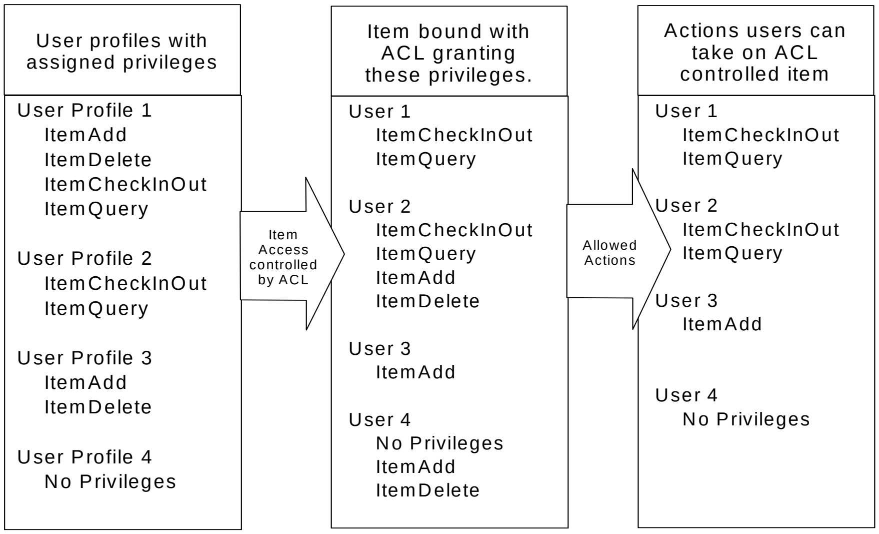
- Item Type
- Item
- Both Item and Item Type
- At the Library Level

By default, *Public access enabled* is turned on and allows access to system default services like the *NOINDEX* item type.

Note: If *Public Access* is disabled, the system will rebuild compiled ACL tables recreating all table views. All ACLs that specify *Public Access* will be ignored during the access control list process.

When a user takes action on an item controlled by an access control list, the system compares the privileges assigned to the user in the user's assigned privilege set to the privileges granted the user in the ACL controlling the item. Even though the ACL may grant the user additional privileges beyond their user profile defined privileges, the user will only be able to perform actions where there are matches between the user profile privileges and the ACL privileges granted the user. If the user has privileges defined in their assigned privilege set that are beyond what is contained in the ACL controlling the item, those privileges (or actions) cannot be taken on the controlled item.

Access control lists restrict privileges and do not grant added privileges. (See Figure 5–8 for an example of the interaction between user assigned privileges and access control lists assigned to an item.)



User profiles with assigned privileges	Item bound with ACL granting these privileges.	Actions users can take on ACL controlled item
User Profile 1 ItemAdd ItemDelete ItemCheckInOut ItemQuery	User 1 ItemCheckInOut ItemQuery	User 1 ItemCheckInOut ItemQuery
User Profile 2 ItemCheckInOut ItemQuery	User 2 ItemCheckInOut ItemQuery ItemAdd ItemDelete	User 2 ItemCheckInOut ItemQuery
User Profile 3 ItemAdd ItemDelete	User 3 ItemAdd	User 3 ItemAdd
User Profile 4 No Privileges	User 4 No Privileges ItemAdd ItemDelete	User 4 No Privileges

Figure 5–8 *Access Control List Privileges*

In Figure 5–8, user 1 has the privileges for adding, deleting, checking in / out, and query / retrieving items. Because the ACL assigned to the desired item only allows user 1 to check in / out and query / retrieve the item, user 1 will not be a able to add or delete an item. Likewise, user 4 has no privileges assigned in their user profile, but the ACL grants user 4 item add and delete capability. An ACL cannot increase the default privileges assigned in a user profile so user 4 still has no privileges to take action on the controlled item. Notice in the above example, user 2 even though granted add and delete privileges in the ACL will still only have check in/out and query/retrieve privileges for the controlled item. User 3 has their user profile defined privileges further restricted by the ACL, so they will only be able to add an item. Content Manager provides the following pre-configured access control lists, (see Table 5–7).

Table 5–7 *Content Manager Default ACLs*

Default Access Control List	Predefined purpose for the access control list
SuperUserACL	Content Manager default ACL for the Content Manager predefined user profile ICMADMIN. This ACL is not displayed and essentially matches all the privileges (AllPrivSet) assigned to the ICMADMIN user profile. This ensures all actions can be performed on all Content Manager ACL bound entities.
NoAccessACL	Default ACL containing a single rule that specifies for all Content Manager users (public). No actions (NoPrivSet) are allowed on the item for which this access control list has been assigned.
PublicReadACL	Default ACL assigned to all users providing read access. Consists of a single rule that specifies that all Content Manager users are granted public access (ICMPUBLC) with read capability (ItemReadPrivSet) for the protected item. When user profiles are created, this is the default that is assigned unless it is overwritten.
DocRouteACL	Default ACL consists of a single rule that specifies that all Content Manager users are granted public access (ICMPUBLC).

Privilege sets define an individual's maximum ability to use the system. An ACL restricts that individual's access to an item. ACLs define the authorization of the bound entities like items and do not circumvent the users defined privileges. For example, if its ACL allows the photograph item to be deleted but the user does not have the delete privilege in his privilege set, then the user cannot delete the photograph.

Create an Access Control List

1. ___ Expand **Authorization**.
2. ___ Highlight **Access Control List**. Create a **New ACL**.
3. ___ Type **Photos** for the name. Provide a description if you desire.
4. ___ **Select all the administrative domains** to Photos can be used in each.
5. ___ Under Find group/users select **Show All**.
6. ___ Locate and highlight the **PhotoLabAdmin** name.
7. ___ Under the Privilege Sets, **highlight SysAdminSubDomainCM**.
8. ___ Select **ADD**.

   Notice that the user to privilege set match is added to the ACL.
9. ___ Select the **Groups** radio button.
10. ___ Highlight the **PhotoLabUsers** group.
11. ___ Highlight the **ClientUserAllPrivs** privilege set.
12. ___ Select **ADD**.

    You have now added a user and group of users to the access control list. Remember that both users **PhotoLabAdmin** and **PhotoTech** belong to the **PhotoLabUsers** group. It would seem to be a conflict in the access control list having assigned both the **PhotoLabAdmin** directly to a privilege set and then the **PhotoLabUsers** group. When the user attempts to perform an action on an item, the privileges assigned in his user profile are compared to those granted in the access control list. The precedence is as follows:

- privileges in the user profile,
- privileges assigned directly to the user in the access control list,
- and then privileges assigned to a group in the access control list.

    If the user is included in multiple groups, then the union of the privileges assigned to each group represent the privileges compared to the privileges assigned in the user profile to determine item access. At all levels the user still cannot perform an action that does not exist in his originally assigned user profile privilege set.

13. ___ Select **OK**, to save the Access Control List.

    Now that the ACL has been saved, it can be assigned to item types, parts, users, and document routing entities. You will use the access control list in later exercises.

Before leaving this section, review Table 5–8 for tables that are involved with access control lists.

Table 5–8 *Library Tables Containing Access Control Information*

Table Name	Purpose
Access Control List Code Table (ICMSTAccessCodes)	Maintains the access control list identifiers. Each list is uniquely identified by the AccessListCode. The list specifications are stored in the access control list table (ICMSTAccessLists). ACL name and description are defined in the NLS Keywords Table (ICMSTNLSKEYWORDS).
Domain Access Control List Code Table (ICMSTDomainAccess)	Maintains associations of Access Control List Codes with the domain. Rows with the same DomainID form a domain's access control list code.
Access Control List Table (ICMSTAccessLists)	Maintains the access control list specifications. A list can contain more than one control. Each control is composed of two elements: **who** (user ID, UserKind) can perform **what** (PrivSetCode). Each Content Manager data entity (Item) must be bound to a control list. The control specifications will then be enforced whenever Items are accessed.
Compiled ACL Table (ICMSTCompiledACL)	Contains the compiled access control information. The user ID contains only individual users. The PrivDefCode represents a single Privilege for Item access. For incremental refresh on this table, please refer to section *Access Control Compilation* paragraph *Incremental Refresh*.
Compiled Permission Table (ICMSTCompiledPerm)	Contains the compiled individual user's User Privileges. The user ID contains only individual users. The PrivDefCode represents a single Privilege for Item access.

Item Access Process

The diagram in Figure 5–9 should assist in understanding how privileges are reviewed and access granted to protected items.

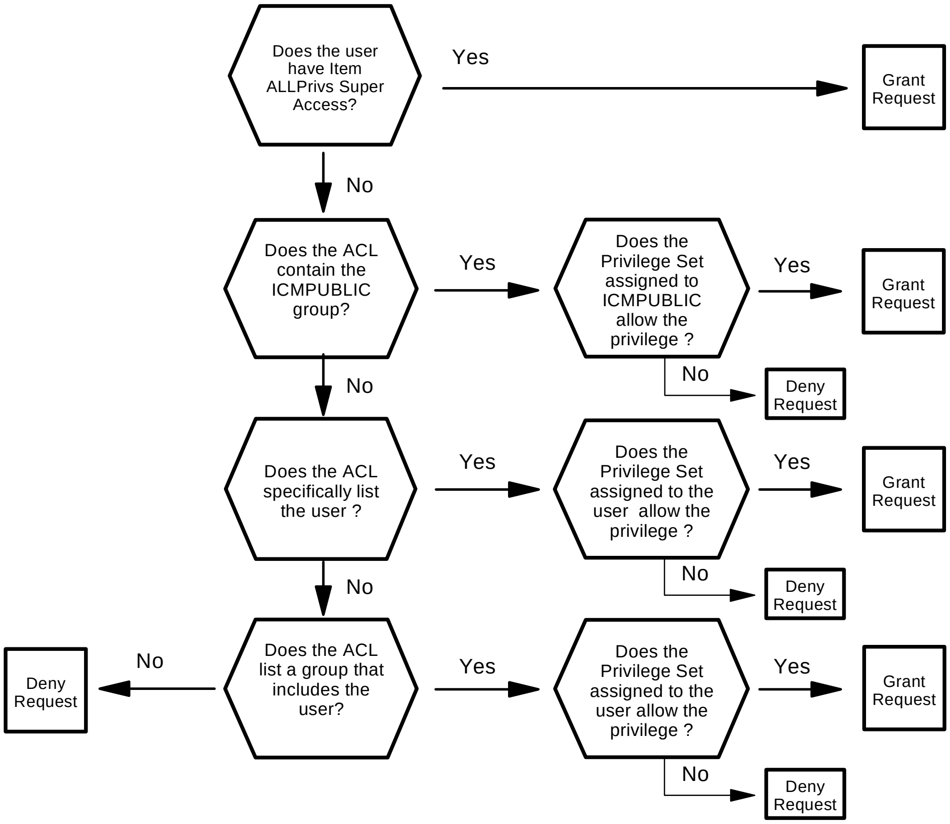

Does the user have Item ALLPrivs Super Access?
Yes
Grant Request
No
Does the ACL contain the ICMPUBLIC group?
Yes
Does the Privilege Set assigned to ICMPUBLIC allow the privilege ?
Yes
Grant Request
No
Deny Request
No
Does the ACL specifically list the user ?
Yes
Does the Privilege Set assigned to the user allow the privilege ?
Yes
Grant Request
No
Deny Request
No
Deny Request
No
Does the ACL list a group that includes the user?
Yes
Does the Privilege Set assigned to the user allow the privilege ?
Yes
Grant Request
No
Deny Request

Figure 5–9 *Example of How Privilege Sets and Access Control Lists Work*

The access control process first checks to see if the user is a super user like the *ICMADMIN* with all privileges. If yes, then the action is granted. Next the process checks to see if public access has been granted in the Library Server configuration and checks the assigned ACL. Next, the system checks to see if the user is listed in the ACL and finally the system checks the groups listed in the ACL to see if the user is a member. In both cases the user must have the privilege in his user profile privileges to take the action.

Summary

In Content Manager Version 8.1 the system security has been enhanced by adding Administrative Domains allowing the user administrative task to be assigned to sub or departmental administrators. The basic premise still holds that users are assigned a set of privileges in their user profile and those privileges represent the maximum rights they have to take action on objects stored in the system. What was added in version 8.1, was the ability to define in the user profile the maximum privileges the user can grant to other users they create so that sub administrators could not grant greater privileges than what they own or a reduced set than what they own if the overall system administrator prefers.

In Content Manager, it still holds that Access Control Lists (ACL) are used to define the maximum privileges that can be performed on a stored object by the indicated uses or groups of user. The ACL does not grant the user rights beyond what they already have in their user profile. So, even if the action is permitted in the ACL, if the user does not have the right they still cannot take the action on the object.

C H A P T E R 6

Defining the Data Model

- Creating Attributes
- Building Item Types
- Defining Child Components
- Setting up Auto-Foldering
- Reviewing Links and References

One of the big benefits of Content Manager version 8.1 is the newly defined data model. Previous releases had a flat data model centered around Index Classes defined by their attributes. The Index Class was used to define and store all items in the system. Documents, images, and other objects were stored as parts of the item defined by the Index Class. An item without parts was also used to represent folders. A subset of the Index Class attributes could also be defined to limit user access to certain attributes. The new model continues many of these benefits, but adds the flexibility to have hierarchal child components. The Index Class is now an Item Type that can have child components. This section will provide steps for setting up the data model for a sample PhotoLab.

Content Manager Version 8.1 extends this model by re-casting Index Classes as Item Types. Added to the item type is the ability to define multiple levels of child components containing multi-valued attributes. In addition, the item type can now contain links and references to resources and other item types so information can be included within an item type without replication. The item type also has the enhanced feature of providing foreign keys. Often solution providers or application integrators have their own application built on a database and want to integrate with Content Manager in a way where the data from their application can be referenced by Content Manager. The foreign key allows an item type attribute to be linked to another item type attribute or a database table column. The data in the target attribute or database table column can be used to validate data being entered into an attribute.

Within the Content Manager System Administration client the following data modeling items are listed.

- Attributes
- Attribute Groups
- Reference Attributes
- Item Types
- Link Types
- MIME Types
- Semantic Types
- Media Object (XDO) Class

Other enhancements like foreign keys are contained within the item type definition and are not listed as an entity under the System Administration Client data modeling area. Not all of the data model enhancements are used in the Content Manager Windows Client or eClient. Some of the enhancements like links, references, and foreign keys have been added to further support the building of solutions on the Content Manager base. This section will cover the areas of the data model focusing specifically on those used by the Content Manager clients. To begin, the first thing that is needed is to define the attributes used in the system. The desired attributes will be used to create item types required for storing content into Content Manager. You will continue with the PhotoLab example in this section.

Defining Attributes

The first step in setting up item types for storing objects into Content Manager is to define the attributes that will be used to hold the data (metadata) and values that describe the object (documents, images, videos, etc.). These attributes are used in searches and queries from within the Content Manager clients and line of business applications to locate stored content. Once an attribute has been defined, it can be used in multiple defined item types. Because of this, it is recommended that attributes be setup as simply as possible to represent data and to allow re-use in multiple item types.

Content Manager ships with a number of default system attributes that can be used in item types along with those you define. The intent of this section is to create an item type named PhotoLab with the following attributes: Account, Customer, Address, Phone, Category, Cost, Date Received, Date Ready and Comments. Think of a scenario where you have a PhotoLab hosting digital photos and videos being worked on for different constituents.

1. ___ Start the *System Administration client* by selecting **Start | Programs | IBM Content Manager for Multiplatforms V8.1 | System Administration**

2. ___ Specify the default user ID **ICMADMIN** and password as **password**.

3. ___ Highlight and expand **Data Modeling** to reveal the data modeling areas.

4. ___ Select **Attributes** and create a new attribute.

   Table 6–1 shows the available Content Manager attribute Types. All can be used in item types, but the BLOB and CLOB are intended for line of business applications and are not supported by the Content Manager Windows Client or the eClient. They are provided here to show how the attributes are represented through the Content Manager API interface.

Table 6–1 *Content Manager Attribute Definitions*

Description	Constant	Object
BLOB (Binary large object)	DK_CM_BLOB	bytes[]
Character	DK_CM_CHAR	java.lang.String
CLOB (Character large object)	DK_CM_CLOB	java.lang.String

Table 6–1 *Content Manager Attribute Definitions*

Description	Constant	Object
Date (YYYY-MM-DD)	DK_CM_DATE	java.sql.Date
Decimal	DK_CM_DECIMAL	java.math.BigDecimal
Double	DK_CM_DOUBLE	java.lang.Double
Long integer (whole numbers -2147483647 to 2147483647)	DK_CM_INTEGER	java.lang.Integer
Short integer	DK_CM_SHORT	java.lang.Short
Time (HH.MM.SS)	DK_CM_TIME	java.sql.Time
Time stamp	DK_CM_TIMESTAMP	java.sql.Timestamp
Variable character	DK_CM_VARCHAR	java.lang.String

5. ___ Type **Category** for the attribute name.

In our PhotoLab scenario, this will be used to identify different types of photos such as: cars, landscape, space, videos, and others.

8.1

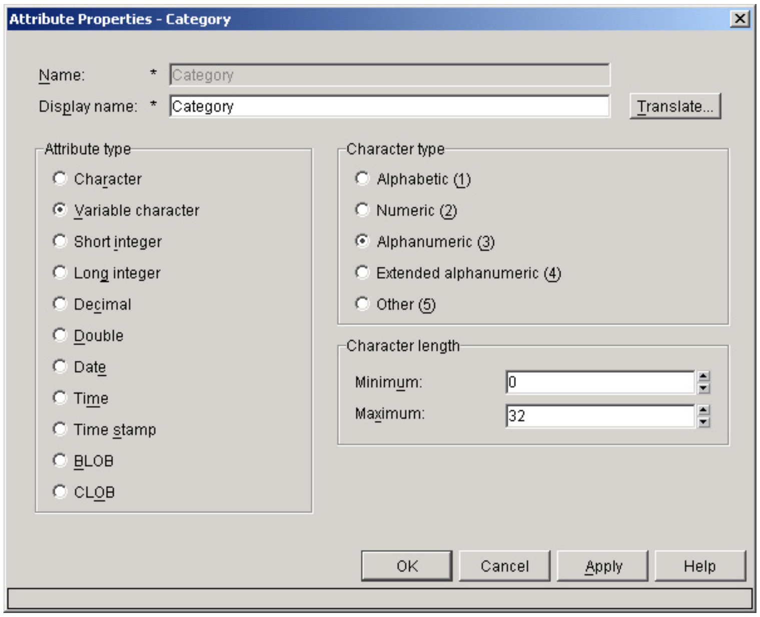
> **Note:** Notice the *Translate* push button for the Display Name. Remember that the attribute name represents the attribute in the database and cannot be changed. The Display Name can be changed and can also be translated to other languages for use within Content Manager clients and integrated solutions.

6. ___ Select an attribute type of **Variable character**.

7. ___ Select a Character type of **Alphanumeric**.

8. ___ Set the Character length at **Minimum = 0 and Maximum = 32**.

The attribute screen should look like Figure 6–1.



Attribute Properties - Category

Name: * Category

Display name: * Category

Attribute type

○ Character
● Variable character
○ Short integer
○ Long integer
○ Decimal
○ Double
○ Date
○ Time
○ Time stamp
○ BLOB
○ CLOB

Character type

○ Alphabetic (1)
○ Numeric (2)
● Alphanumeric (3)
○ Extended alphanumeric (4)
○ Other (5)

Character length

Minimum: 0

Maximum: 32

Figure 6–1 *New attribute properties screen*

9. ___ Select **OK**, to save the Category attribute.

10. ___ Use Table 6–2, to add the remaining attributes for the Photolab item type. Take notice of the different defaults and ranges for the attributes being added.

Table 6–2 *Attributes for the PhotoLab Item Type*

Name	**Attribute Type**	**Character Type**	**Length**	**Use**
Account	Long Integer		Take defaults	Used for customer account number.
Customer	Variable character	Alphanumeric	Minimum = 0, Maximum = 32	Used to identify the owner of the photos.
Address	Variable character	Extended alphanumeric	Minimum = 0, Maximum = 32	Customer street address, city, state.

Table 6–2 *Attributes for the PhotoLab Item Type*

Name	Attribute Type	Character Type	Length	Use
Phone	Variable character	Extended alphanumeric	Minimum = 0, Maximum = 15	Customer phone number.
Order Number	Short Integer		Take defaults	Identifies customerÕs individual order.

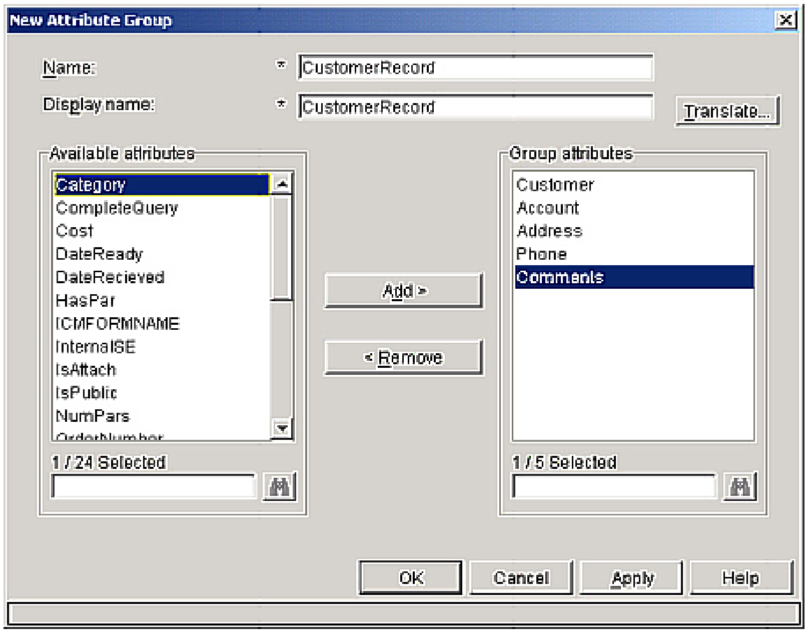
Cost	Decimal		Total=10
			Fixed=2
				Charge for photo development.

Date Received	Date			Date order was submitted.
Date Ready	Date			Date photos were ready.
Comments	Variable character	Extended alphanumeric	Minimum = 0, Maximum = 50	Comments concerning the order.

Using Attribute Groups

Attributes may be used in multiple item types. For convenience in assigning correlating attributes to item types, one can create an Attribute Group. For example, if each of the item types in your system uses the same attributes for a customer reference, then it makes sense to include the customer name, address, phone, etc., in an attribute group. This will save time in the future when creating item types.

1. ___ Highlight **Attribute Groups** and create a New Attribute Group.
2. ___ Type **CustomerRecord** for the name.
3. ___ Add **Customer, Account, Address, Phone, and Comments** to the group as shown in Figure 6–2.



Name: * CustomerRecord

Display name: * CustomerRecord

Available attributes

- Category
- CompleteQuery
- Cost
- DateReady
- DateRecieved
- HasPar
- ICMFORMNAME
- InternalSE
- IsAttach
- IsPublic
- NumPars
- OrderNumber

1 / 24 Selected

Group attributes

- Customer
- Account
- Address
- Phone
- Comments

1 / 5 Selected

Figure 6–2 *Creating an Attribute Group*

4. ___ Select **OK** to save the Attribute Group.

> **Note:** Nested attribute groups are not allowed. You cannot assign an attribute group when adding a group.

Adding Reference Attributes

A reference is a single direction one-to-one association between the root or child component of an item (item type) to the root component of another item (item type) as shown in Figure 6–3. Once created, the reference can be included into the attribute listing of the source item type. When this is done, the delete rule of the reference can be selected from one of the following options: No action, Restrict, Cascade, or Set Null.

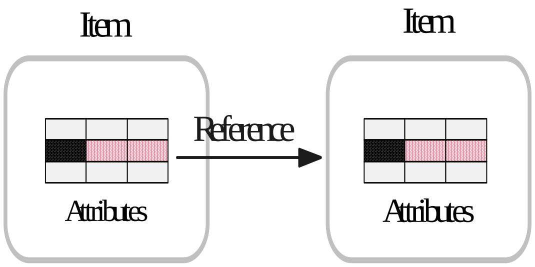
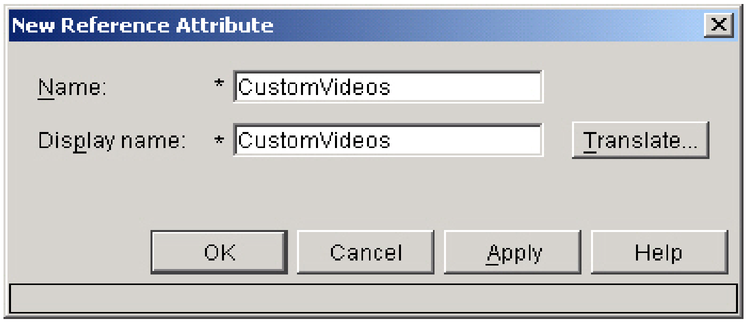


Figure 6–3 *Reference attribute from one item to the root of another*

In the PhotoLab scenario, you have customers with photo processing accounts that will be represented in an item type. The PhotoLab customer satisfaction department could also have an item type to cover customer complaints. Instead of including all the customer information in the complaints item type, a reference could be used. For the stated order complaint there is a single customer. For the complaint, there is an order reference.

1. ___ Highlight **Reference Attributes** and select new.

2. ___ Type **CustomVideos** for the name, see Figure 6–4.



Name: * CustomVideos

Display name: * CustomVideos

Figure 6–4 *Creating a reference attribute*

3. ___ Select OK, to save the new Reference.

Note: References have been added for use within integrated solutions built on the Content Manager base. References are not exposed through the Content Manager clients. Keep this in mind when creating item types for use with the Content Manager clients.

Later in this section you will see how the reference shows up in the item type. For more information on references, refer to *Modeling Your Data in Content Manager version 8.1*.

Creating Link Types

Content Manager added links so that defined item types can be linked at the root component (root level of the item). This means the link relationship is between selected common attributes defined at the root level of each item type (see Figure 6–5). Attributes defined at the child levels (components) in the item type cannot be used for link relationships. The purpose of the link is to allow the content of an item type to be linked to another item type to avoid copying the resources into the second item type when needed.

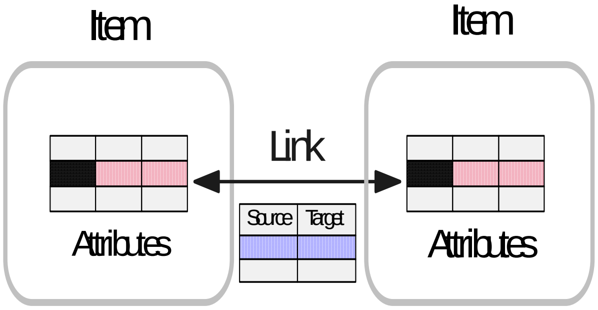


Figure 6–5 *Link between two items held in links table*

An example of linking is the auto-foldering support in Content Manager. An item type is created for users to import images. This item type has what is called base parts so imported objects can be stored. A second item type is created to represent the folder, but without document part definitions. A single common attribute between the item types is used to setup the auto-link. Now when users import objects into the first item type, users who have access to the item type representing the folder can search the system and locate objects imported with the first item type.

In the PhotoLab scenario, a link could be used between the customer record and the photo processing order using the account attribute for the link. This would allow orders to be entered into the order item type using the account attribute to link back to the customer record. Doing this allows those taking orders to take the customers order without repeating the customer information in the order item type.

As a default, Content Manager provides two default link type definitions.

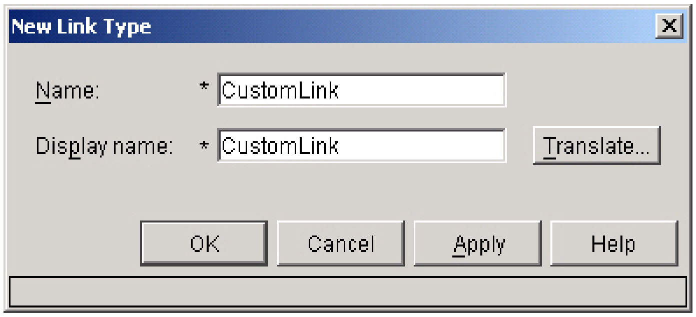
- **DKFolder** (Folder contains): Default used for auto-foldering to mimic the connection between a physical folder and document contained in a folder.

- **Contains** (containment relationship): A link where each item's resource appears to be contained in the linked item.

When links are established, the resources for each item type are still managed as independent entities. The links table in the Library Server database maintains the relationship between linked items. For the purposes of this study guide, the following steps will define the link shown in Figure 6–6, but it will not be used with the Content Manager clients. The Content Manager clients do not support links beyond auto-foldering. When item types are defined later in this section the folder containing a link will be used for auto-foldering.

1. ___ Highlight **Link Types** and select new.

2. ___ Type **CustomLink** for the name.



Name: * CustomLink

Display name: * CustomLink

Figure 6–6 *Creating a link type*

3. ___ Select **OK**, to save the new link type.

> **Note:** Links have been added for exploitation within integrated solutions built on the Content Manager base. Links are not exposed through the Content Manager clients other than for auto-foldering. This needs to be considered when creating item types for use with the Content Manager clients.

Later in this section links in the item type will be demonstrated. For more information on links, refer to *Modeling Your Data in Content Manager version 8.1*.

Creating Media Object (XDO) Classes

The *media object class* is used to specify system actions that can be performed on core object types stored on Content Manager associated resource managers. When defined, the object is associated with a defined attribute group allowing the object class to inherit the system defined attributes for the object type, (see Figure 6–7 on page 185). The Java class is included, along with the specific server side DLL or shared object for handling the object. A media object class needs to be defined before the object type can be associated to an item type. The predefined media object classes in Table 6–3 are sufficient to handle most Content Manager implementations.

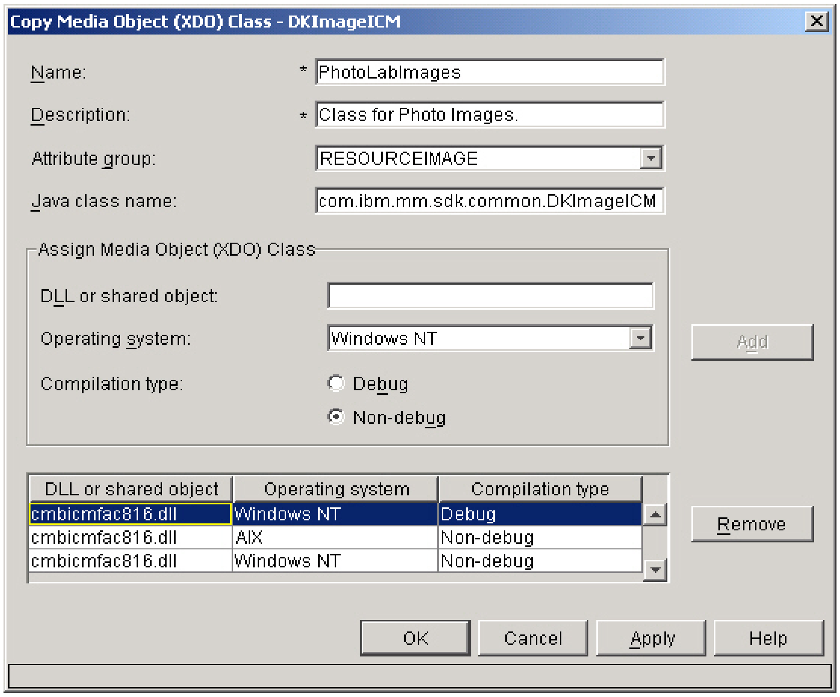
Table 6–3 *Predefined Media Object Classes*

Default Part	Default purpose for the part
DKImageICM	Specific object class handler used for Binary Larger Objects (BLOB) stored on a Resource Manager. This class has been deprecated and is provided for compatibility with prior releases.
DKLobICM	The base media object class handler used to add, retrieve, update, and delete generic large objects (LOB) stored on a Resource Manager. Any object can be stored using this class despite the MIME type.
DKStreamICM	Specific large object handler designed to add, store, and update (synchronously or asynchronously) generic streamable data stored on a Resource Manager. This is actually a subclass of DKLobICM.
DKTextICM	Specific object class handler used to add, retrieve, update, and delete text based parts stored on a Resource Manager where the content needs to be indexed for textual searches. This is actually a subclass of DKLobICM.
DKVideoStreamICM	Specific object class handler used to initiate a streaming session for content stored on an external video server (Resource Manager) like Content Manager VideoCharger. This is actually a subclass of DKLobICM that inherits the methods of DKStreamICM.

The following steps will demonstrate setting up a media object class that will be used later in this section to define a document part.

1. ___ Highlight **Media Object (XDO) Classes**.
2. ___ Highlight the media class named **DKImageICM**.
3. ___ Select **Copy**.

This will display the media object class definition screen.



Copy Media Object (XDO) Class - DKImageICM

Name: * PhotoLabImages

Description: * Class for Photo Images.

Attribute group: RESOURCEIMAGE

Java class name: com.ibm.mm.sdk.common.DKImageICM

Assign Media Object (XDO) Class

DLL or shared object:

Operating system: Windows NT

Compilation type: ○ Debug ● Non-debug

DLL or shared object	Operating system	Compilation type
cmbicmfac816.dll	Windows NT	Debug
cmbicmfac816.dll	AIX	Non-debug
cmbicmfac816.dll	Windows NT	Non-debug

Figure 6–7 *Media object (XDO) class definition screen*

4. ___ Type **PhotoLabImages** for the name.

5. ___ Type **Class for Photo Images** for the description.

6. ___ Notice the **RESOURCEIMAGE** attribute group is selected so the new media object class will inherit or use the system defined attributes allocated for handling images or BLOBs.

7. ___ Notice the **Java class name** and assigned **DLL and Shared Object** to handle the objects of this class on the designated servers.

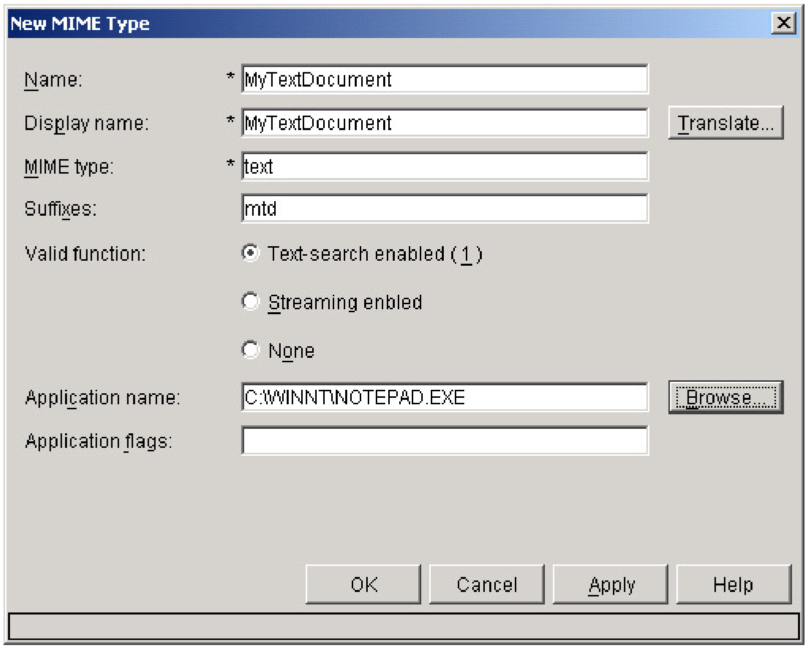
8. ___ Select **OK**.

Adding MIME Types

Adding a *MIME type* is necessary when documents, images, photos, and other objects added to Content Manager do not have a predefined default. The MIME type is a registered Internet standard describing the content of the object and the application that generated the object. This includes identifying the different extensions or suffixes that might represent the object. This allows the object or file to be handled correctly as long as there is an object handler that understands the specific MIME type of the object. All files or objects stored in Content Manager need to have their MIME type identified so Content Manager clients and other applications correctly handle the object.

1. ___ Highlight **MIME Types**.

2. ___ Select **New** to display the MIME type definition screen, (see Figure 6–8).



Name: * MyTextDocument

Display name: * MyTextDocument

MIME type: * text

Suffixes: mtd

Valid function: ● Text-search enabled (1)
○ Streaming enbled
○ None

Application name: C:\WINNT\NOTEPAD.EXE

Application flags:

Figure 6–8 *MIME type definition screen*

3. ___ Type **MyTextDocument** as the name.

4. ___ Type **text** as the MIME Type.

5. ___ Type **mtd** as the suffix.
6. ___ Select **Text Search Enabled** under valid functions.
7. ___ Select **c:\winnt\notepad.exe** for the application name.
8. ___ Select **OK**.

For further practice, use the Windows client to import files assigning an extension of “mtd” and selecting the MyTextDocument as the file type.

8.1

Note: The MIME type just defined should show up in the ICMSTMIMETYPES Library Server table.

Adding Semantic Types

A *semantic type* is a descriptive attribute that assists applications in identifying the behavior (semantics) for specific types of items. For example a document item type without parts can be used to represent a folder and a document item type with parts can be used to store documents. Integrated solutions and the Content Manager clients use the semantic types to correctly classify a newly created item. By doing this the nature of the item can be distinguished in queries performed by the Content Manager clients and integrated solutions. Table 6–4 describes the Content Manager predefined semantic types.

Table 6–4 *Predefined semantic types*

Semantic Type	**Default purpose for the semantic type**
Annotation	Represents the annotation parts in Content Manager.
Base	Refers to the stored base part for an item.
Container	Generic reference used for handling items that contain parts.
Document	Describes a document with base parts (ICMBASE) that may or may not have annotations and notelogs.
Folder	For use in handling folders containing items or other folders.
History	Provides for migration from earlier Content Manager systems to handle the history log.
Note	Describes the notelog of information maintained as part of an item using the document model.

For installations where Content Manager is used as an enterprise document management or imaging system, using the Content Manager clients, the predefined semantic types are sufficient and not directly exposed to users. Integrated solutions built on Content Manager may need to define additional semantic types to represent the objects used in their solution. Semantic types will not be used in the exercises of this section.

Creating Item Types

Item types are used as templates for defining and categorizing items created in Content Manager. This includes the template definitions for stored objects like documents, images, and other files. Item types replace the term and function of *Index Classes* in previous Content Manager releases. When users import or scan using the Content Manager clients, they select the item type that will define the stored object. When the desired item type has been selected, the user is presented the attributes defined in the item type to describe the object being stored. The clarifying attribute information (metadata) is stored in attribute tables along with the item reference in the Library Server database. Likewise, users using the Content Manager clients, or integrated solutions, perform searches or queries against the item type using the defined attributes to locate stored objects. Table 6–5 lists the predefined item types shipped with Content Manager.

Table 6–5 *Predefined item types shipped with Content Manager*

Predefined item types	Default purpose for the item type
NOINDEX	Default item type used by the Content Manager clients for importing and scanning objects. Item type contains source, user ID, and timestamp attributes. It also contains the following document parts required by the Content Manager clients: ICMANNOTATION, ICMBASE, and ICMNOTELOG. Access control is public read.
ICMSAVEDSEARCH	Default item type used by the Content Manager clients to handle queries. Access control is public read.
ICMFORMS	Default item type for form overlays used by the Content Manager Clients. This resource item type has a single variable character extended alphanumeric attribute and uses a Media Object Class of DKLobICM. Access control is public read.

Before setting up an item type, it is helpful to understand the different ways an item type can be defined.

Item Type Classifications

When item types are created in Content Manager they need to be classified to assist Content Manager in determining the purpose for the item type.

Content Manager provides four default item type classifications: item, resource, document, and document part.

8.1

Note: This is especially important when using the Content Manager Windows Client or eClient which only support the document item type.

Item

The classification of *item* represents items in the system that do not have associated parts like documents, images, photos or files. The attributes contained in the item type are sufficient to describe the purpose for the item and represent the content for the item, (see Figure 6–9). In the PhotoLab scenario, an item type classified as item could be used to store customer or account information. This essentially stores all the data in the Library Server database without associated parts on the Content Manager Resource Manager.

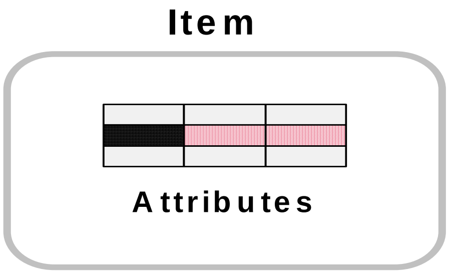


Figure 6–9 *Item classified as item*

The item type classification of item is not supported in the Content Manager clients. The benefit of having an item type classification like *item* is in the support of integrated solutions. Independent software vendors and solution providers can use this item type classification to define information used in their solution where the data is contained totally within the database tables used by the Library Server.

Resource

The classification of *resource* represents items in the system that do have associated parts like documents, images, photos or files stored on a Resource Manager. The attributes contained in the item type should describe or clarify the stored resource files. In the PhotoLab scenario, a resource item type of photo orders could have attributes describing the order (reference customer, order number, etc.) and then point to the photo portfolio on the Resource Manager that comprises the order, (see Figure 6–10).

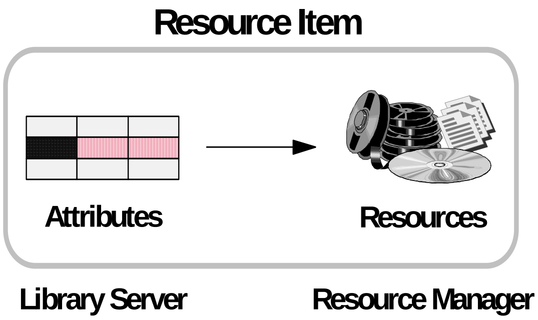


Figure 6–10 *Item classified as a resource item*

The item type classification of resource is not supported in the Content Manager clients. The benefit of having an item type classification like this is in the support of integrated solutions. Independent software vendors or solution providers can use the resource item type classification to build compound document management or internet solutions where the application stores reference data (metadata) on the Library Server linked to objects stored on the Resource Manager.

Document

The classification of *document* is provided to model an enterprise document management system or a historical imaging system. This is the only item type classification supported by the Content Manager Windows Client and eClient. The model is similar to previous releases of IBM ImagePlus and IBM Content Manager providing the default base, notelog, and annotation parts, (see Figure 6–11 on page 192) needed by the Content Manager clients. Two additional default parts are provided. The first (ICMBASESTREAM) to facilitate storing videos and the second (ICMBASETEXT) intended for documents targeted primarily for text indexing. For multi-part documents, the attributes stored on the Library Server apply to all the document parts residing on the Resource Manager.

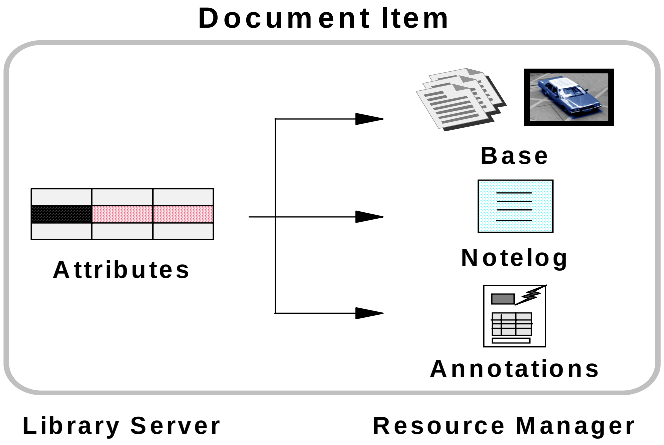


Figure 6–11 *Item classified as a document item*

The document item type classification allows the document management default parts shown in Table 6–6 on page 193 to be selected and linked to the item when creating an item type. An item type of document can be created using the default parts or no associated parts. For example, to represent a folder that can be used with the IBM Content Manager clients, create a document item type with attributes and no associated document management parts. This will be done later in this section. Essentially, this does the same thing as creating an item type of item, but an item type of item cannot be used with the IBM Content Manager clients.

It is important that integrated solutions that share content stored in Content Manager with the Content Manager clients follow the item type document model. For example, a front end batch capture solution should store the scanned images as ICMBase parts in an item based on the document item type. Doing this allows the attributes stored for the item to be used in searches by the Content Manager clients and the images stored as base parts to be displayed in the clients. In cases where the front end batch scan system wants to also index information that has been OCR'ed (Optical Character Recognition) from the images, the OCR'ed text file can be stored as an ICMBASETEXT part. The indexed information can then be used to locate the item. Likewise, using the ICMBASESTREAM for storing videos provides a nice way of storing videos so the Content Manager clients can locate the videos and then launch a defined video player to handle the videos.

Document Part

In some implementations the predefined default document management parts shown in Table 6–6 may not be sufficient to handle what an integrated solution requires. In these cases, Content Manager provides the capability to define additional document management parts using an item type template. To create a document part item type, the document part classification is selected and then the desired Media Object (XDO) Class has to be assigned to represent the document part, see Table 6–6 for a list of predefined default Media Object Classes. Once this is done, the document part item can be saved and then used as an associated part when creating item types based on the document classification.

Table 6–6 *Predefined default parts for document item type*

Default Part	Default purpose for the part
ICMBase	The fundamental part of the document item type used to store documents, images, photos, or any object stored in the system.
ICMBaseText	Like the ICMBase part. Used for storing textual type documents or files that are intended to be indexed for full text searches.
ICMBaseStream	Like the ICMBase part. Used for storing videos that can be used with Content Manager VideoCharger.
ICMNotelog	Used to store the information added to the item notelog in the Content Manager clients.
ICMAnnotations	Used to hold the markups (sticky notes, color highlights, stamps, or other graphical highlights) added to objects in the Content Manager when using the Content Manager clients.

Creating a Document Part Item Type

This section will provide the steps for creating a document part item type. The goal is to show how the part can be created and then used when creating item types classified as documents.

1. ___ Before creating an item type, create a file system directory named **C:\IDX**. This will be used later in the example steps.
2. ___ Highlight **Item Types** and select new.

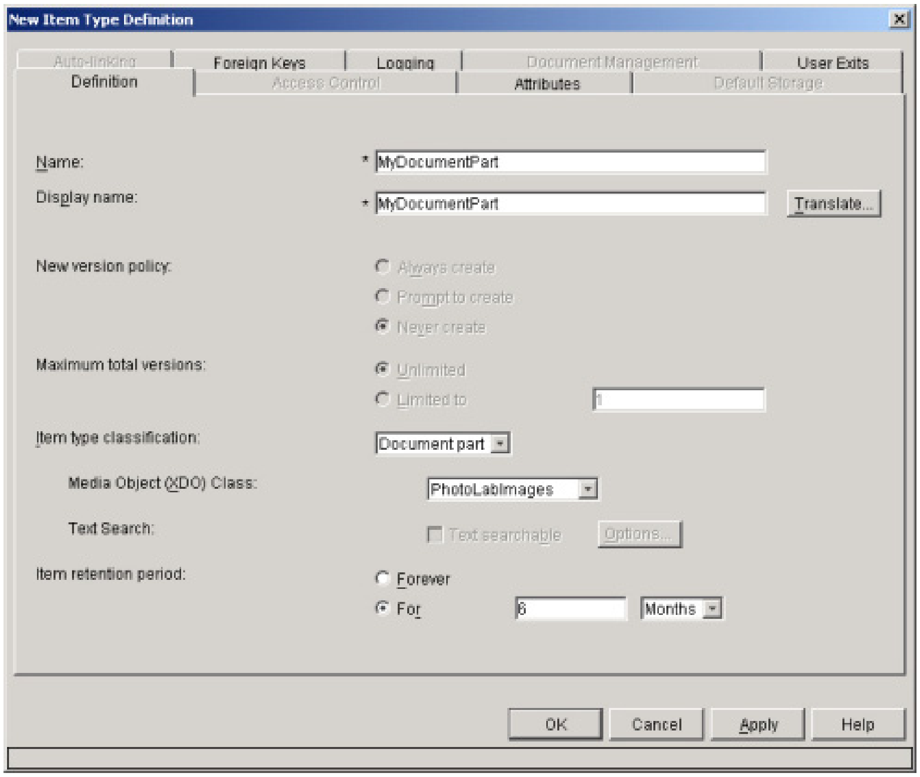
3. ___ Select the **definition** tab.

4. ___ Use Table 6–7 to complete the entry fields on the new item type definition tab.

Table 6–7 *Options for the document part item type definition*

Definition field	Data or option
Name	MyDocumentPart
Item type classification	Document Part
Media Object Class	PhotoLabImages
Text Search	Select the text searchable check box.
Item retention period	Select **For** and type 6 months.

5. ___ Select the **Media Object (XDO) Class** and notice that all of the predefined and user defined media classes are listed.



Name: * MyDocumentPart

Display name: * MyDocumentPart

New version policy: ○ Always create ○ Prompt to create ● Never create

Maximum total versions: ● Unlimited ○ Limited to 1

Item type classification: Document part

Media Object (XDO) Class: PhotoLabImages

Text Search: □ Text searchable

Item retention period: ○ Forever ● For 6 Months

Figure 6–12 *Document part item definition screen*

6. ___ Select the **PhotoLabImages** media class created in the previous sections of this chapter.

7. ___ Notice the **Text Searchable Options** has been disabled. It would be enabled if DKTextICM or a media class that derives its definition from DKTextICM had been selected.

8. ___ The definition tab screen should resemble Figure 6–12.

9. ___ For now ignore the other item type tabs.

   Because this is an item type definition, default attributes can be assigned to the part along with the linking to another item or database table using a foreign key. This option will be covered in a later section.

10. ___ Select **OK** to save the document part.

As the next item type is created, you will see how this document part can be used in an item type.

Creating a Document Item Type for Folders

In order to use the auto-foldering capability in the Content Manager clients a document item type needs to be created to represent the folder. Creating an item type classified as item will not work for the Content Manager clients, but would be applicable for integrated solutions where the Content Manager clients are not to be used. To handle auto-foldering an item type needs to be created with attributes that match the item type used to import the stored objects.

1. ___ Highlight **Item Types** and select new.
2. ___ Type **MyPhotoWork** for the item type name.
3. ___ Take the defaults for the rest of the options on the *item type Definition* screen.
4. ___ Select **Access Control**.
5. ___ Make sure the **Access Control** is set to **PublicReadACL**.\
6. ___ Select **Attributes**.
7. ___ For attributes, add **Customer, Account, Address, Phone and OrderNumber**.

   Note the above should reinforce that given the time, our PhotoLab scenario could be split out with different item types to represent the customer information, the order information, and processing information. Using references and links to connect the data avoids information duplication in each item type. In this case a single attribute is being used for the link, the remaining attributes for query fields.

8. ___ Take the default options after adding each of the attributes.
9. ___ Select **OK** to save the item type**.**

   An error message will be displayed indicating that an item type without any parts is being created and that the full function of the clients will not be available. This means objects cannot be stored into this item type. This is not a problem for the folder item type.

10. ___ Select **Yes** to accept the error and save the item type.

Creating a Document Item Type

Carrying on with the PhotoLab scenario, the following steps will create an item type for use in later exercises. As this item type is created, the following steps will point out different options on each of the item type definition dialogue tabs. Some of the options may not be used in this item type as they may not be supported by the Content Manager clients used in later labs. It is important that the item type be setup as described.

1. ___ Highlight **Item Types** and select new.

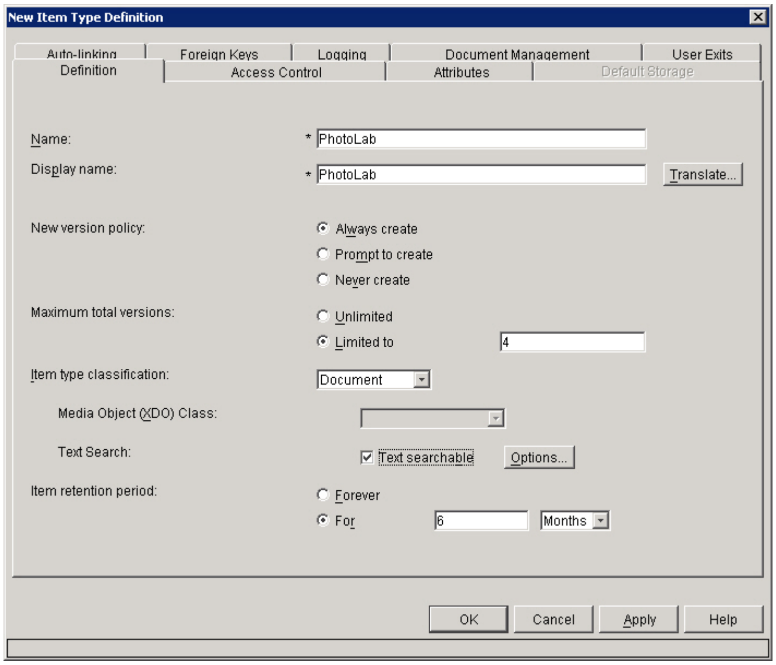
Item Type Definition

2. ___ Use Table 6–8 to complete the entry fields on the item type definition tab.

Table 6–8 *Exercise options for item type definition dialog*

Definition field	Data or option
Name	PhotoLab
New version policy	Always create
Maximum total versions	Limited to 4 (After 4 the oldest will be deleted)
Item type classification	Document
Text Search	Select the text searchable check box.
Item retention period	Select **For** and type **6** months.

3. ___ The *New Item Type Definition* screen should resemble Figure 6–13 on page 198.



Name: * PhotoLab

Display name: * PhotoLab

New version policy: ● Always create ○ Prompt to create ○ Never create

Maximum total versions: ○ Unlimited ● Limited to 4

Item type classification: Document

Media Object (XDO) Class:

Text Search: ☑ Text searchable

Item retention period: ○ Forever ● For 6 Months

Figure 6–13 *Item type definition used in PhotoLab*

4. ___ Notice the **Versions options**.

8.1

Note: The Content Manager version support allows the entire item type to be versioned, the individual document management part, and / or the attributes defined for the item type. This provides the ability to have a persistently defined item while tracking the modifications in the document parts. In this scenario, after four versions the oldest version of the item will be deleted.

5. ___ The **Item retention period** provides support for items to be retired or removed after a stated period of time. The services on the server for handling the removal of retired items will be added in future releases.

6. ___ Notice the Document Management tab is enabled when document classification has been selected. Notice also that **Media Object (XDO) Class** cannot be selected, because the document classification assumes predefined document parts.

Text Search Indexing Options

7. ___ Select text searchable **Options**.

8. ___ Use Table 6–9 to update the **Text Search Options**:

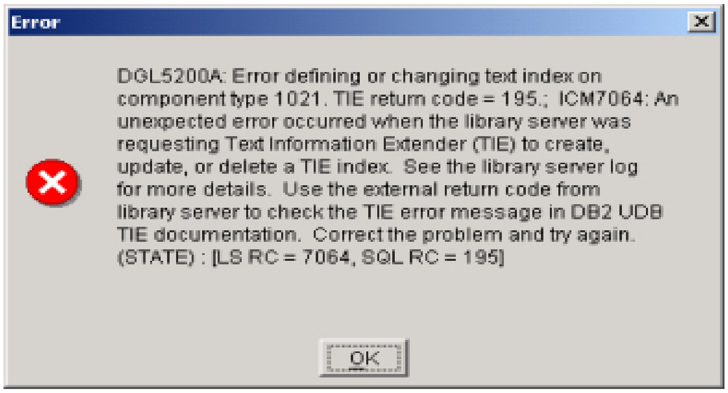
Table 6–9 *Choices for the text search options screen*

Text Search Option	Data	Purpose
Format	Text	Format of the text to be indexed.
CCSID	850	Supported code page.
Language	EN_US	Language code used to create indexes.
Index Directory	c:\idx	Location on the server where index files are stored.
Working Directory	c:\idx	Location on the server for the temporary working files.
User Defined Function	ICMfetchContent	User defined functions for interpreting the text to be indexed. Two predefined functions are defined. ICMfetchContent for indexing the content of text files and ICMfetchFilter for indexing converted text like from IBM Lotus WordPro. If self-defined functions are used then the schema or data layout should also be specified.
Changes before Update	0	Changes made before the index is updated. Should never be this low on an operational system.
Update every	5 minutes	Frequency or time lapse between the index being updated. Used for this exercise, should be higher for operational systems.
Commit Count	Take the blank default.	Number of updates performed before the index if committed.

9. ___ Take the remaining defaults on the screen.

10. ___ Select **OK** to save changes to the **Text Search Options**.

In order for the text search options to be updated the DB2 Text Information Extender must be active. If not, then an error will be displayed when the item type is saved. This is because the actual text search options are committed to the server when the item type is saved, not when the Text Search Options screen is exited. If an error is encountered indicating a problem with DB2 Text Information Extender, the first thing that should be checked is to make sure Text Information Extender has been started. Second, check the Library Server configuration setting to make sure the user ID and password is correct for DB2 Text Information Extender. Once these have been verified, the error message return code will have to be used to troubleshoot the problem using the DB2 Text Information Extender logs.



DGL5200A: Error defining or changing text index on component type 1021. TIE return code = 195.; ICM7064: An unexpected error occurred when the library server was requesting Text Information Extender (TIE) to create, update, or delete a TIE index. See the library server log for more details. Use the external return code from library server to check the TIE error message in DB2 UDB TIE documentation. Correct the problem and try again. (STATE) : [LS RC = 7064, SQL RC = 195]

Figure 6–14 *Error displayed when the text search index or working directories entered do not match existing directories on the server.*

In addition, errors are written to the System Administration Client dklog.log and the server icmserver.log error files. For more information on text search options and error codes, refer to the *DB2 Text Information Extender Administration and User's Guide Version 7.2*

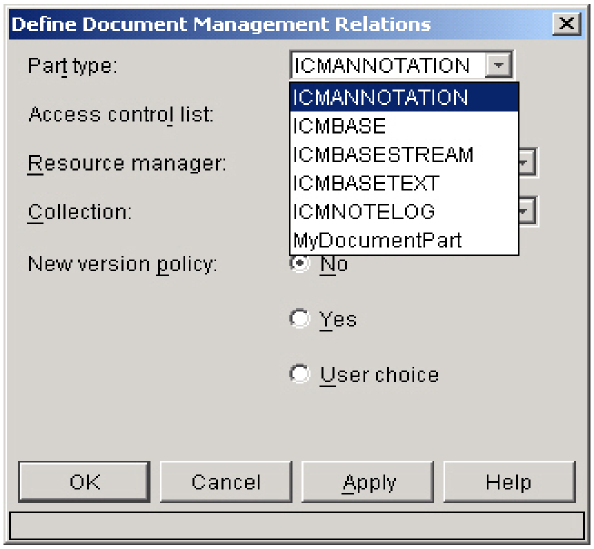
Note: The error displayed in Figure 6–14 is an actual error from typing the incorrect index and working directories on the server. The directories must first exist on the server before being used as they will not be created from the entered text.

Item Type Document Management

11. ___ Select **Document Management**.

12. ___ Select **Add**.

13. ___ Select the **Part Type** drop down list box to see a list of defined parts.



Define Document Management Relations

Part type: ICMANNOTATION

New version policy: ● No ○ Yes ○ User choice

Figure 6–15 *Document Management parts that can be assigned to an item type.*

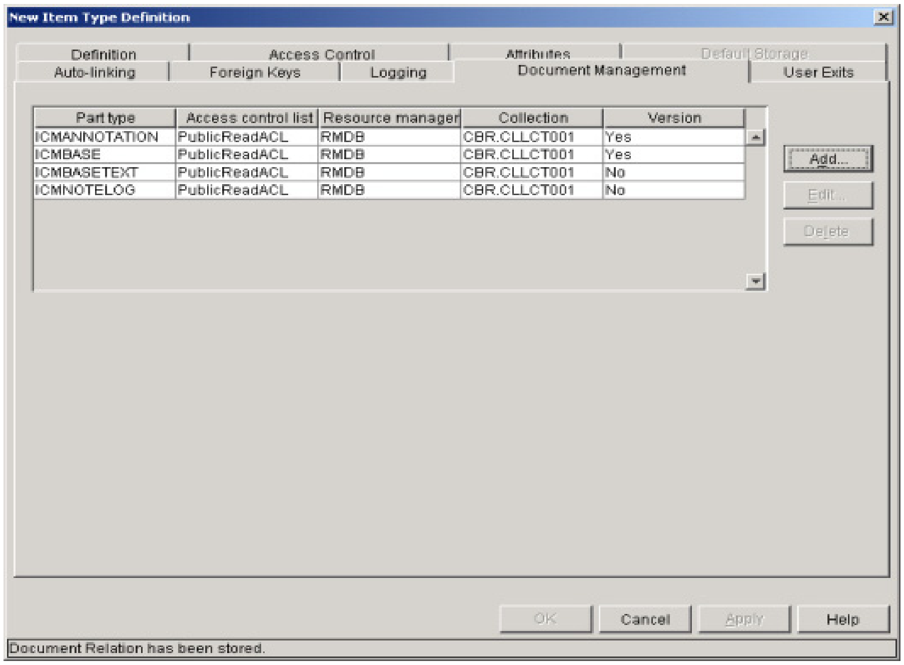
14. ___ Notice in Figure 6–15 the part **MyDocumentPart** is listed and could be selected as a base part. Notice also that if MyDocumentPart was selected for addition, then the version policy could be selected at this time. For the following exercises, the Content Manager predefined defaults will be used.

15. ___ Add the parts shown in Table 6–10. Take the default Resource Manager.

Table 6–10 *Document parts added to PhotoLab item type*

Document Part	Access Control List	Collection	Version Policy
ICMAnnotation	PublicReadACL	CBR.CLLCT001	Yes
ICMBase	PublicReadACL	CBR.CLLCT001	Yes
ICMNotelog	PublicReadACL	CBR.CLLCT001	No
ICMBaseText	PublicReadACL	CBR.CLLCT001	No

16. ___ The document parts screen should look like Figure 6–16 on page 202.



Part type	Access control list	Resource manager	Collection	Version
ICMANNOTATION	PublicReadACL	RMDB	CBR.CLLCT001	Yes
ICMBASE	PublicReadACL	RMDB	CBR.CLLCT001	Yes
ICMBASETEXT	PublicReadACL	RMDB	CBR.CLLCT001	No
ICMNOTELOG	PublicReadACL	RMDB	CBR.CLLCT001	No

Document Relation has been stored.

Figure 6–16 *Document parts assigned to item type*

Item Type Access Control

17. ___ Select the **Access Control** item type tab.

18. ___ The access control should be set to **PublicReadACL.**

You could have used the Photos ACL created during the Access Control exercise in the chapter on *Managing System Access*. That ACL was setup giving all users ClientUserAllPrivs which would suffice for actions the users would perform using the Content Manager clients. Because the labs throughout this guide assume the default Content Manager user ID, the predefined ACLs will be used.

19. ___ The access control list checking should be set at the **item type level**.

Each item added to the system using this item type template will be constrained by the same access control list.

Item Type Attributes

The *item type attributes* definition screen provides the capability to assign attributes at the root level (root component) of the item or to one or more child levels. Child levels or child components are a grouping of attributes defined below the root level of the item type. Child components are needed to implement multi-valued attributes that were defined in earlier releases of Content Manager. The item type supports multiple child components at multiple levels in the item type definition hierarchy. This is beneficial for integrated solutions working with compound document or web objects that require multi-level object definitions. For the Content Manager clients, only the first level of child components are supported.

20. ___ Select the **Attributes** item type tab.

21. ___ Highlight the following attributes using the keyboard CTRL and the left Mouse Select button: **Customer, Account, Address, Phone, and Category**.

22. ___ Select **Add** to list the attributes under the *Selected Attributes and Components* area.

Note: This essentially adds the attributes to the root level or root component of the item type.

23. ___ Use the attribute move buttons, (see Figure 6–17) to order the list as indicated above.

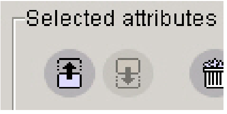
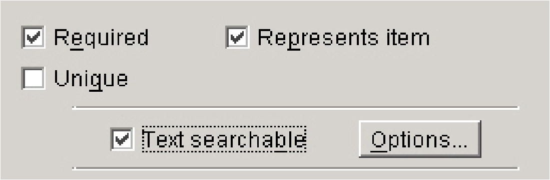


Figure 6–17 *Item type attribute move buttons*

24. ___ Highlight **Customer** in the *Selected Attributes* area, (see Figure 6–18) and select the following: required, represents item, and text searchable.



☑ Required ☑ Represents item

□ Unique

☑ Text searchable Options...

Figure 6–18 *Item type attribute settings*

25. ___ Select the **Text searchable** options. Use Table 6–9 on page 199 to complete the text search options.

8.1 **Note:** Making the attribute text searchable allows the attribute text to be indexed. Using the Client for Windows, contents can be selected for the attribute search on the basic search screen.

26. ___ Locate under *Available attributes or groups* **CustomerRecord**.

This group contains the same attributes that were just added to the item type. Normally assigning the group would be a more convenient means of adding the attributes. Unfortunately, the Content Manager Windows Client does not expose the attributes in a group making it difficult to add attribute information. This is not seen as a permanent restriction, but for now if the Windows client is to be used refrain from using groups.

27. ___ The desired attribute and attribute groups can be created while working within the item type by selecting the options shown in Figure 6–19.

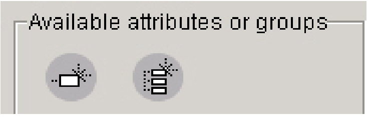


Figure 6–19 *Item type create attributes and groups*

Item Type Child Component Attributes

Item type supports creating child component or attribute levels at multiple imbedded levels. This exercise will only create attributes at the first child level so the child component can be used with the Windows client. Following the PhotoLab scenario a child component will be created to contain the orders for the customer. Because the customer has multiple orders, you want the attributes to be multi-valued and in order for this to happen there must be a child level item. Another way this could have been done is to set up an individual item type for orders using links or references to connect the two. In this case each order would be an individual item.

28. ___ Highlight **OrderNumber**.

29. ___ Select **Add/New Child**.

30. ___ Type **Order** for the *Child Component Name*.

31. ___ Leave the delete rule set at **Cascade**.

8.1

> **Note:** Cascade allows the root or item to be deleted if child levels have been defined. Restrict requires that the child component levels be deleted prior to deleting the root level item.

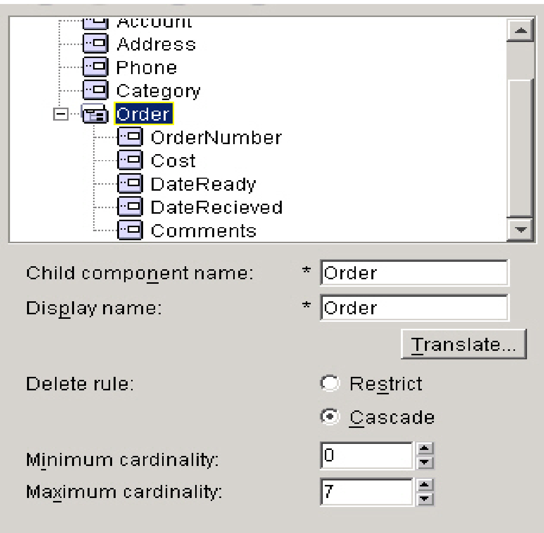
32. ___ Set the **Maximum cardinality to 7**. Leave the minimum set to 0.

8.1

> **Note:** Cardinality defines the minimum and maximum number of child components that can be defined.

33. ___ With the child level **Order** still highlighted, select and add the following attributes: **Cost, Date Received, Date Ready, Comments**. List the attributes in this order under Order.

34. ___ Highlight **Comments** under Order and select **Text Searchable**.



- Account
- Address
- Phone
- Category
- Order
  - OrderNumber
  - Cost
  - DateReady
  - DateRecieved
  - Comments

Child component name: * Order

Display name: * Order

Translate...

Delete rule: ○ Restrict ● Cascade

Minimum cardinality: 0

Maximum cardinality: 7

Figure 6–20 *Item type child level attributes*

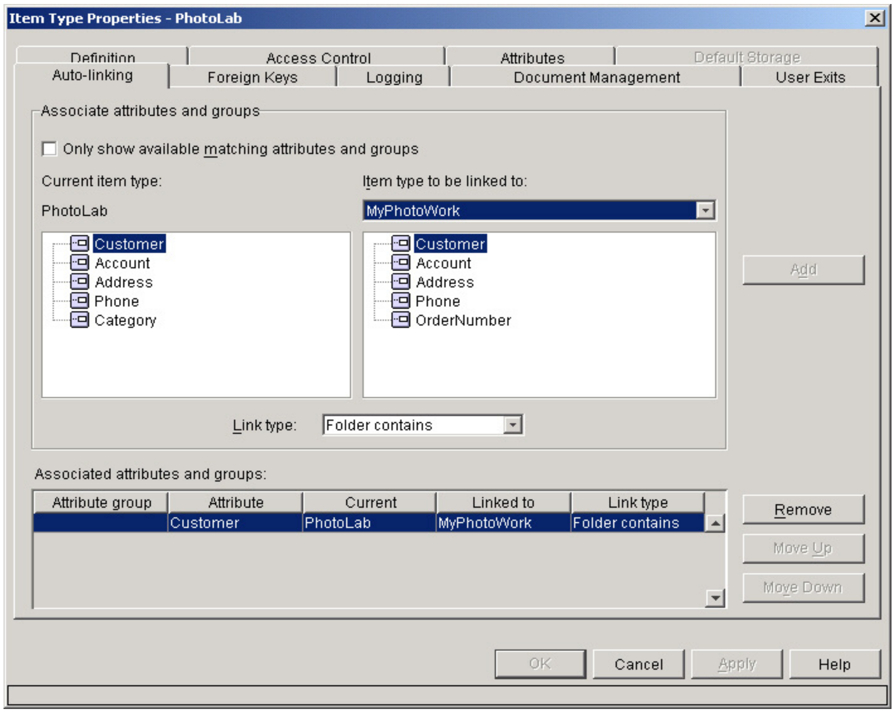
35. ___ The child level attributes should look like Figure 6–20.

Before closing and saving the item type additional item types options need to be selected and reviewed.

Item Type Auto-Linking

Auto-linking must be used to replicate the auto-foldering capabilities of earlier Content Manager releases. The auto-link must be established in the item type used for importing the objects. The link can only be established in a single attribute. This attribute cannot be a decimal.

1. ___ Select the **Auto-Linking** tab.
2. ___ Highlight **MyPhotoWork** in the *Item Type to be linked to* drop down.
3. ___ Highlight **Customer** in *PhotoLab*. **Customer** should automatically be selected in *MyPhotoWork*. If not select **Customer**.
4. ___ The *Link Type* should be **Folder Contains**, see Figure 6–21 on page 207.
5. ___ Select **Add**.
6. ___ Now try to link account. The system will only let you link a single attribute for auto-foldering
7. ___ Expand the *Link Type* and you should notice the **CustomLink**, (see Figure 6–21) created earlier in this chapter.



Associate attributes and groups

☐ Only show available matching attributes and groups

Current item type: PhotoLab

Item type to be linked to: MyPhotoWork

Customer
Account
Address
Phone
Category

Customer
Account
Address
Phone
OrderNumber

Link type: Folder contains

Associated attributes and groups:

Attribute group	Attribute	Current	Linked to	Link type
	Customer	PhotoLab	MyPhotoWork	Folder contains

Figure 6–21 *Item type auto-linking an attribute*

Before closing this item type there are a few additional areas to review.

Item Type Foreign Keys

A *foreign key* is used to link the attribute definition in an item type to the attribute definition in another item type or an external database table column. The foreign key is supplied by the underlying database to provide referential integrity between the item type attribute and the target item type attribute or table column. This is handy for line of business applications that would like to compare or validate attribute entries with a list of predefined attribute values in a database column or another item type. Foreign keys are not exposed through the Content Manager Clients.

1. ___ Select the **Foreign Keys** tab.

2. ___ Select **Add**, (see Figure 6–22 on page 208).

3. ___ Select a **Source Attribute**.

4. ___ Under *Select target item type or table*, select **Use external table.**

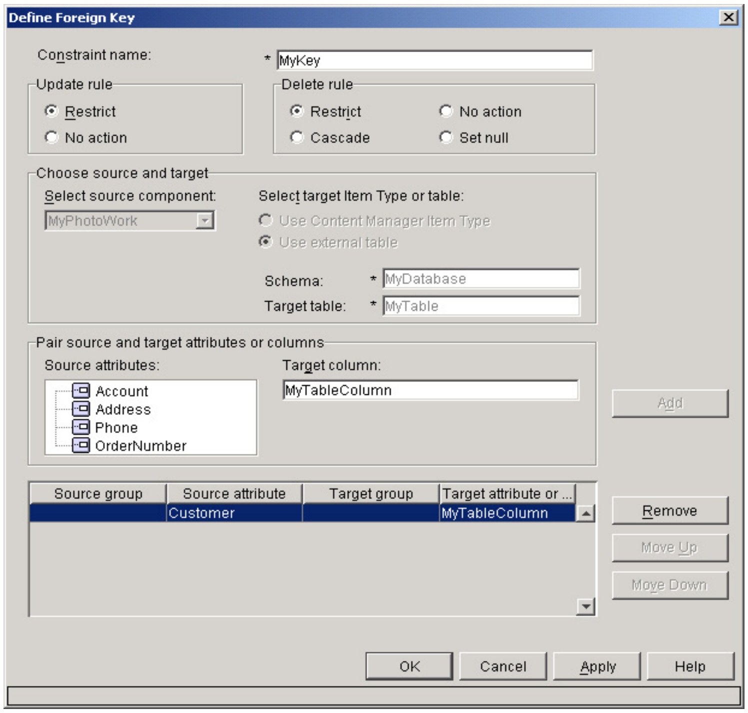
5. ___ Type **MyDatabase** for the *schema*.

6. ___ Type **MyTable** for the *table*.

7. ___ Type **MyTableColumn** for the *table column*.

8. ___ Select **Add** to list the *foreign key link*.

9. ___ At this time the *Define Foreign Keys* screen should resemble Figure 6–22.



Define Foreign Key

Constraint name: * MyKey

Update rule: ● Restrict ○ No action

Delete rule: ● Restrict ○ No action ○ Cascade ○ Set null

Choose source and target

Select source component: MyPhotoWork

Select target Item Type or table: ○ Use Content Manager Item Type ● Use external table

Schema: * MyDatabase

Target table: * MyTable

Pair source and target attributes or columns

Source attributes: Account, Address, Phone, OrderNumber

Target column: MyTableColumn

Source group	Source attribute	Target group	Target attribute or ...
	Customer		MyTableColumn

Figure 6–22 *Item type foreign key definition screen*

10. ___ Note instead of selecting an **External table**, *Use Content Manager item type* could have been selected to do a foreign key match on the attributes in two item types.

11. ___ Select **Cancel**.

You do not want to save the foreign key in this item type as foreign keys will not be used in later labs.

Item Type Event Logging

One enhancement in Content Manager involves the ability to log events for actions taken on an item defined per the item type definition. The events are logged in the Library Server events tables. Instead of turning on logging for all items created across all item types, targeted item types can be selected to monitor use.

___ Select the **Logging** tab.

8.1

Note: The events that can be logged are when an item is created, read, updated, or deleted.

Item Type User Exits

Within the item type, *user exits* for the Content Manager Windows Client can be enabled by specifying the desired function and DLL containing the function. These are client side exits to alter default user actions when searching, sorting, and saving items. A Resource Manager client user exit is also available to alter the collection for stored items.

___ Select **OK** to save the *Item Type*.

At this point the required item type for the PhotoLab scenario has been created. You have a PhotoLab item type for storing objects and a MyPhotoWork item type for use as a folder in accessing objects stored in PhotoLab. The steps for importing objects into the defined item types are covered in the chapter on Content Manager *Client for Windows, Importing Using an Item Type.*

Create an Item Type Subset

An *item type subset* is a restricted view of the attributes added to an item type. Users using the Content Manager clients can be restricted to using the subset for access to the attributes in the defined item type. This gives a company the capability to block sensitive data from employees that may not have a need to access the information. Added to the subset support in Content Manager Version 8.1 is the ability to also filter based on the content of the attributes the user is allowed to view. This essentially filters the rows of data returned to the user when doing an attribute search. Use the following steps to setup an item type subset for PhotoLab.

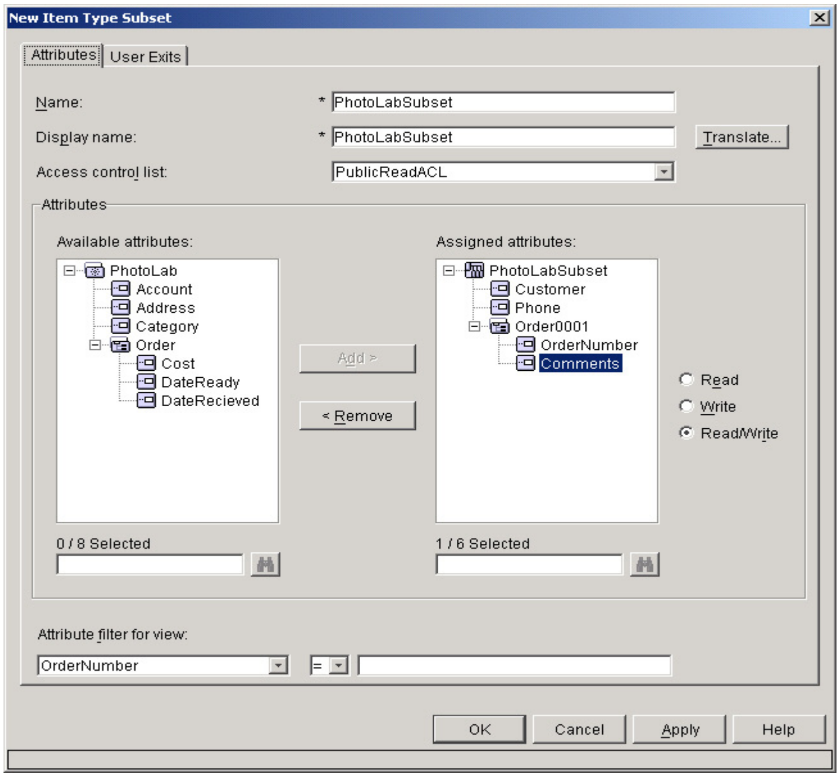
1. ___ Highlight and expand the **PhotoLab Item Type.**
2. ___ Highlight **Item Type Subset** and select **new**.
3. ___ Type **PhotoLabSubset** as the name.
4. ___ Select **PublicReadACL** as the *Access Control List*.
5. ___ From the **Available Attributes** area assign the attributes listed in Table 6–11 to the **Assigned Attributes** selecting the indicated action.

Table 6–11 *Actions allowed for assigned attributes*

Assigned Attribute	Action
Customer	Read
Phone	Read
OrderNumber	Read
Comments	Read/Write

6. ___ In Figure 6–23 notice at the bottom of the screen the **Attribute filter for view**.
7. ___ Each of the *Assigned Attributes* can have a further filter applied by adding an acceptable text string that the subset is allowed to view. Leave **blank**.

Note: When defining a subset for an item type with root and child levels, at least one attribute from the root level must be assigned to the subset before an attribute from the child level can be assigned. This is the case with each subsequent child level.



New Item Type Subset

Attributes | User Exits

Name: * PhotoLabSubset

Display name: * PhotoLabSubset

Access control list: PublicReadACL

Attributes

Available attributes:

- PhotoLab
  - Account
  - Address
  - Category
  - Order
    - Cost
    - DateReady
    - DateRecieved

0 / 8 Selected

Assigned attributes:

- PhotoLabSubset
  - Customer
  - Phone
  - Order0001
    - OrderNumber
    - Comments

1 / 6 Selected

○ Read
○ Write
● Read/Write

Attribute filter for view: OrderNumber =

Figure 6–23 *Item type subset definition screen*

8. ___ Select **User Exists** and notice that the subset provides the capability to invoke an exit on searching and sorting actions.

9. ___ Select **OK**, to save the subset.

To test how subsets work, a specific privilege set and access control list should be created to restrict access to the item type granting users access to the item type subset. Refer to the *System Administration Guide* (SC27-1335) as that is beyond the scope of this study guide. For certification the key is to understand the purpose and use of subsets.

Item Type for VideoCharger Integration

Before leaving the data model area, an item type needs to be created to cover the import of videos during the Content Manager VideoCharger integration section. Use Table 6–12, Table 6–13, and Table 6–14 to complete the item type taking the defaults for the unspecified options.

Table 6–12 *Options for the VideoCharger item type definition dialog*

Field	Data or option
Name	Files
New version policy	Always create
Maximum total versions	Limited to 4 (After 4 the oldest will be deleted)
Item type classification	Document
Text Search	No
Item retention period	Select **For** and type **6 months**.

Table 6–13 *Document parts added to VideoCharger item type*

Document Part	Access Control List	Collection	Version Policy
ICMAnnotation	PublicReadACL	CBR.CLLCT001	Yes
ICMBase	PublicReadACL	CBR.CLLCT001	Yes
ICMNotelog	PublicReadACL	CBR.CLLCT001	Yes

.

Table 6–14 *Attributes for the PhotoLab item type.*

Name	Attribute Type	Character Type	Length	Use
FileName	Variable character	Extended alphanumeric	Minimum = 0, Maximum = 32	Used to hold the video filename.
FileOwner	Variable character	Extended alphanumeric	Minimum = 0, Maximum = 32	Used to hold the video owner’s name.
FileDescrip tion	Variable character	Extended alphanumeric	Minimum = 0, Maximum = 50	Description of the video.

Summary

The expanded data model added to Content Manager Version 8.1 provides extensive enhancements to facilitate the integration of dedicated solutions in the document management, imaging, web content management, and other industries. Building off the flexibility of the item type and extending the data model using child components, references, and links allows solutions to use Content Manager as a middleware content platform. At the same time, the Content Manager clients provide an out of the box enterprise document management/imaging system.

This section has attempted to walk the reader through the main data model areas represented on the certification exam. Extra time should be spent working with the data model features that are beyond the exercises contained in this guide. The certification exam assumes experience with having defined different parts of the data model and having implemented a workable Content Manager Version 8.1 system. Special attention should have been given to the notes included in this section and the relationship of the different features and parts of the data model. The certification exam does cover the parts of the data model that cannot be demonstrated using the Content Manager clients. This guide has attempted to describe these features. However, further study may be needed. Therefore reviewing the *System Administration Guide* (SC27-1335) and the *Modeling Your Data in Content Manager version 8.1* documents that comes with Content Manager is recommended.

CHAPTER 7

Building Document Routing

- Work Nodes
- Workbaskets
- Collection Points
- Worklists

In this chapter, the IBM Content Manager System Administration Client will be used to setup a document routing process. Document routing in Content Manager is a defined process for moving documents and folders from one work node to another work node. A *work node* is a general term to represent work baskets and collection points that are steps in the process where items wait for actions to be taken by the Content Manager clients or integrated solutions. The process consists of at a minimum a starting work node, one action and an ending work node. Work nodes are assigned to a worklist that represent the work packages being moved through the process. The work package contains the item references and associated information (priority, state, resume time, process, etc.) needed to complete the task or action. Worklists are used by the Content Manager clients and integrated solutions to obtain a list of items that need action. The action taken on an item determines whether the item continues through the process, is removed from a process, or started on another process. The steps in this section will setup a document routing process using the PhotoLab item type created in the data modeling section of this guide.

Creating Work Nodes

A *work node* is defined as either a work basket or a collection point. A work basket is a group of documents and folders that are either in process or waiting to be processed. A collection point differs from a workbasket in that its sole purpose is to wait for a specified number of documents within a folder before continuing the process. Once the stated number of documents in a folder are collected, the work package folder is moved down the process to the next work node. User exits can be used to alter the action of the work package upon entering or leaving the work node. In addition, a user exit is provided as an overload limit so action can be taken when the work node has exceeded the number of work packages stated as the limit for the work node. The following steps will setup a document process.

1. ___ Start the **System Administration Client**.
2. ___ Logon using user ID = **icmadmin** and **password**
3. ___ Select **Document Routing** to list the Content Manager document routing components Figure 7–1.

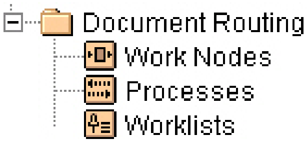


Figure 7–1 *Content Manager document routing components*

The first step in defining a document routing process is to create the work nodes or steps that will comprise the process.

Collection Work Node

A *collection* contains a resume list specifying the number of items, for a given import item type to folder item type match, that must exist in the collection specified folder before continuing the process. Once the stated number of items are collected in the resume list specified folder, the folder work package is moved down the process to the next work node. Figure 7–2 shows the system predefined document routing *start* process with items flowing to a collection work node with a folder resume list waiting for two items.

When using the Content Manager clients, items started on a process during import will flow directly through the collection point to the next work node. Folders started on the process that are not defined in the collection resume list flow directly through the collection to the next work node irrelevant of the number of items in the folder. Folders started on the process that are represented by item types defined in the resume list will remain on the collection work node until the required number of documents or items specified for that folder in the resume list have been met. Once met the folder and contained items represented by the work package proceed to the next work node. The collection work node resume list can have multiple folder item types to required item count matches representing the different item types used for importing objects.

8.1

Note: A collection point only applies to folders started on the process. A folder that is started on a process, defined in the resume list, will wait for a number of items, from the linked item type, specified in the resume list before continuing. Folders not defined in the resume list will proceed directly through the collection to the next work node.

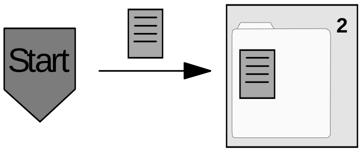


Figure 7–2 *Process predefined start and a collection work node*

1. ___ Highlight **Work Node** and select **New.**
2. ___ On the New Work Node Definition screen, select **Collection Point**.
3. ___ Type **PhotoJobs** for the collection point name.
4. ___ For a description type: **Wait for multiple photos to complete a work package**.
5. ___ Set the Access control list to **PublicReadACL** to match what was used for the PhotoLab item type.
6. ___ Set the **Overload limit** to **5**.

8.1

> **Note:** Overload is the limit of items that the work basket should not exceed. Once hit, processing will continue attempting to use the overload user exit defined function and stated DLL to handle the exception.

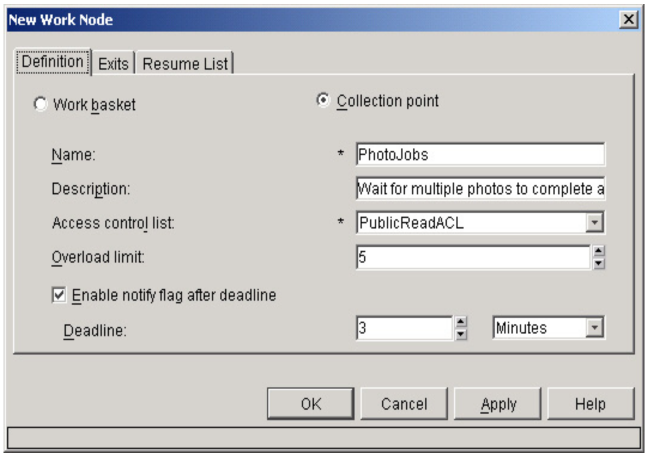
7. ___ Select **Enable notify flag after deadline**.

8.1

> **Note:** The amount of time to wait before users are notified of a passed deadline.

8. ___ Set the deadline to **3 minutes**.

9. ___ The new node definition screen should resemble Figure 7–3.



○ Work basket ● Collection point

Name: * PhotoJobs

Description: Wait for multiple photos to complete a

Access control list: * PublicReadACL

Overload limit: 5

☑ Enable notify flag after deadline

Deadline: 3 Minutes

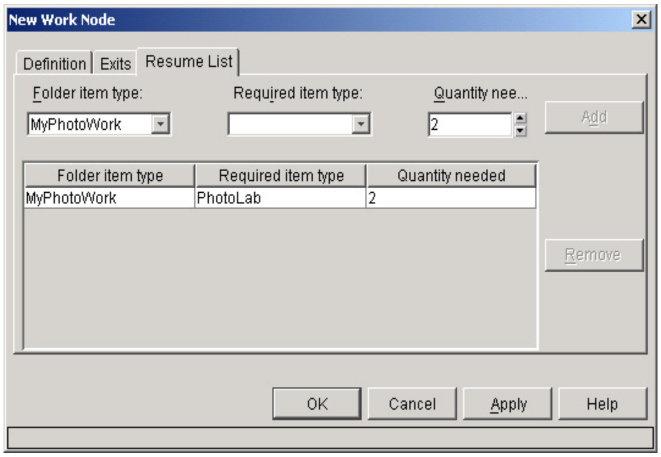
Figure 7–3 *Document routing collection work node*

10. ___ Select **Resume List** to display the resume list screen.

11. ___ Select **MyPhotoWork** as the **Folder Item Type**.

12. ___ Select **PhotoLab** as the **Required Item Type**.

13. ___ Set **Quantity Needed** to **2**.



Folder item type: MyPhotoWork

Required item type:

Quantity nee... 2

Folder item type	Required item type	Quantity needed
MyPhotoWork	PhotoLab	2

Figure 7–4 *Collection work node resume list*

14. ___ Select **Add** to add the collection criteria.

The collection work node resume list should resemble Figure 7–4. Essentially items will be held in the collection node until two items are stored using the PhotoLab item type and then assigned to the document route. The MyPhotoWork folder item type acts as a container with pointers to the items in the process.

Note: You can add additional folder item types and required item type matches to the collection point. Once a required item type has been used, it cannot be re-used.

15. ___ Select **OK** to save the collection work node PhotoJob.

Workbasket Work Node

Workbaskets represent a step in the document routing process that contain work packages awaiting user or application action. The workbasket does not perform actions against contained work packages, but holds the work packages defined in the Library Server database. The work package includes the *itemids* of the documents for which action is needed. Items in the workbasket are represented to the users through Worklists. Figure 7–5 on page 220 shows the document routing process with documents flowing to a workbasket work node.

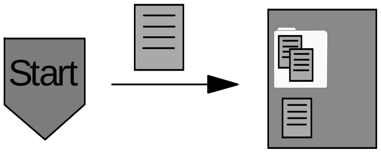


Figure 7–5 *Process predefined start and a workbasket work node*

1. ___ Highlight **Work Node** and select **New.**

2. ___ On the New Work Node Definition screen, select **Workbasket**, (see Figure 7–6).

3. ___ Type **PhotoProcessing** for the workbasket name.

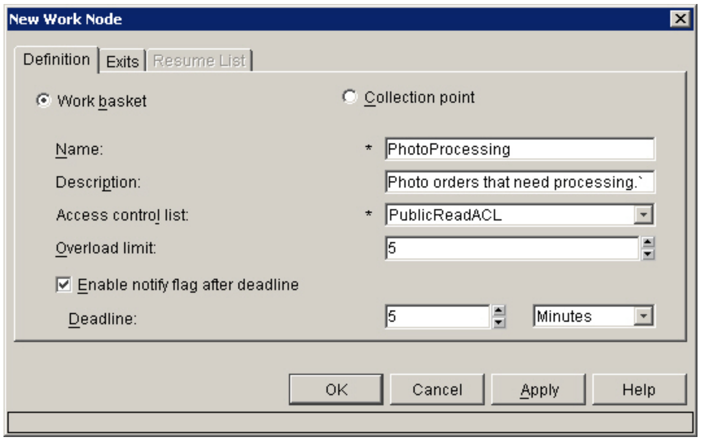
4. ___ For a description type: **Photo orders that need processing.**

5. ___ Set the Access control list to **PublicReadACL**.

6. ___ Set the **Overload limit** set to **5**.

7. ___ Select **Enable notify flag after deadline**.

8. ___ Set the deadline to **5 minutes**.



● Work basket ○ Collection point

Name: * PhotoProcessing

Description: Photo orders that need processing.`

Access control list: * PublicReadACL

Overload limit: 5

☑ Enable notify flag after deadline

Deadline: 5 Minutes

Figure 7–6 *Document routing workbasket work node*

9. ___ Select **OK** to save the workbasket.

10. ___ Now use Table 7–1 and Table 7–2 to create two additional workbaskets.

Table 7–1 *Data for creating a second workbasket work node*

Field	Data to be entered.
Name	PhotoFinishing
Description	Photo orders in the finishing phase
Access Control List	PublicReadACL
Overload limit	5
Deadline	2 Minutes

Table 7–2 *Data for creating a third workbasket work node*

Field	Data to be entered.
Name	PhotoJobProblems
Description	Orders with problems.
Access Control List	PublicReadACL
Overload limit	5
Deadline	2 Minutes

Creating Worklists

You have to create *Worklists* so users using the Content Manager clients, or other solutions, can access the items within the work packages flowing through the process. Work nodes are assigned to a worklist. The worklist represents the work packages contained in the assigned work nodes allowing the contents of the work package to be listed in the worklist by the defining item type. What the user sees are the items in the worklist, by item type definition, that require action, (see Figure 7–7). The assigned nodes can reside in different document routing processes. This gives users with access to multiple document routing processes the ability to reroute items between processes.

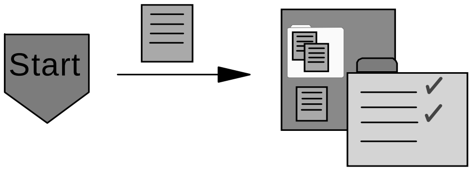


Figure 7–7 *Workbasket work node with a worklist*

1. ___ Highlight **Worklists** and select **New**.
2. ___ Type **PhotoOrders** for the Worklist name.
3. ___ For a description Type **Photo jobs that need processing**.
4. ___ Set the Access control list to **PublicReadACL.**
5. ___ Set **Selection order** to **By date**. Table 7–3 lists the available options for the selection order.

Table 7–3 *Worklist work package selection order*

Selection Order	Worklist actions
By priority	Worklist returns work packages based on priority.
By date	Worklist returns work packages based on the order received in a work node.

6. ___ Leave **Quantity to return** set to **All**.

Allows one to designate whether one, all, or a maximum number of work packages are listed for users accessing the worklist.

7. ___ For the purposes of this study guide, **do not select a Selection filter**. Table 7–4 provides a description of how each filter affects the work packages listed in the worklist the user accesses.

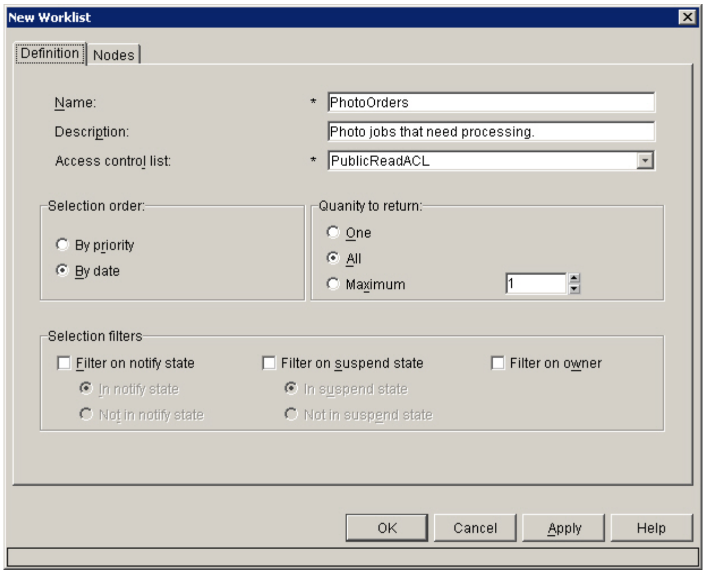
Table 7–4 *Worklist selection filters*

Selection Filters	Options for selection filters
Notify state	Mutually exclusive option to list work packages that are either in a notify state or not in a notify state.
Suspend state	Mutually exclusive option to list work packages that are either in a suspend state or not in a suspend state.
Owner	List work packages based on owner.

8. ___ Select **Nodes**.

9. ___ Add the **PhotoProcessing** work node to the list of *Prioritized nodes in worklist*.

   All of the listed work nodes should be assigned. Both workbaskets and collection work nodes can be assigned to the worklist. In order to demonstrate the document routing process, a single work node for the PhotoLab processing scenario will be assigned to each worklist.



Name: * PhotoOrders

Description: Photo jobs that need processing.

Access control list: * PublicReadACL

Selection order:
○ By priority
● By date

Quanity to return:
○ One
● All
○ Maximum 1

Selection filters
□ Filter on notify state
● In notify state
○ Not in notify state
□ Filter on suspend state
● In suspend state
○ Not in suspend state
□ Filter on owner

Figure 7–8 *Document routing worklist definition screen*

10. ___ Select **OK** to save the worklist depicted in Figure 7–8.

In the photo lab demo scenario, in order to see the photos moving through the process additional worklists are needed.

11. ___ Now use Table 7–5 to create a second work list.

Table 7–5 *Data for the ProcessedPhotos worklist*

Worklist fields	Data for worklist fields
Name	ProcessedPhotos
Description	Processed photo jobs that need finishing
Access control list	PublicReadACL
Selection order	By priority
Quantity to return	All
Selection filters	None
Nodes	Assign PhotoFinishing to prioritized nodes

12. ___ Now use Table 7–6 to create a third work list.

Table 7–6 *Data for the ProblemPhotoJobs worklist*

Worklist fields	Data for worklist fields
Name	ProblemPhotoJobs
Description	Photo jobs that encountered a problem
Access control list	PublicReadACL
Selection order	By priority
Quantity to return	All
Selection filters	None
Nodes	Assign PhotoJobProblems to prioritized nodes

13. ___ Now use Table 7–7 to create a fourth worklist.

Table 7–7 *Data for the PhotoJob worklist*

Worklist fields	Data for worklist fields
Name	PhotoJobs
Description	Photo jobs on the collection
Access control list	PublicReadACL
Selection order	By priority
Quantity to return	All
Selection filters	None
Nodes	Assign PhotoJob to prioritized nodes

With four Worklists created, it will be easier to demonstrate the flow of documents or photos through the document routing process using the Content Manager clients. Notice that for each worklist an Access Control List (ACLs) is assigned. Using ACLs on the worklist provides the security needed to block users from accessing work packages and the items pointed to from within the work package.

Defining a Document Process

With the work nodes created that define the steps in the document process and the Worklists created that users use to access items in the work packages flowing through the process, it is now time to define the process. Content Manager provides two predefined choices to affect how work packages flow through the process. *Continue* can be used to move work packages along the sequential process as users take actions, (see Figure 7–9). *Escalate* can be used to indicate a branch in the process when the user does not take the normal action on an item. The user exits defined for each of the nodes can also affect how a work package is handled when entering and leaving a work node.

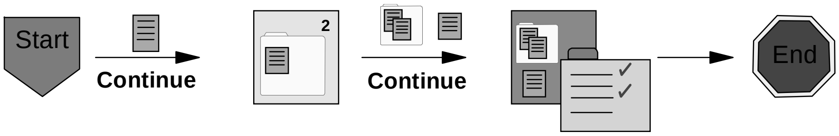


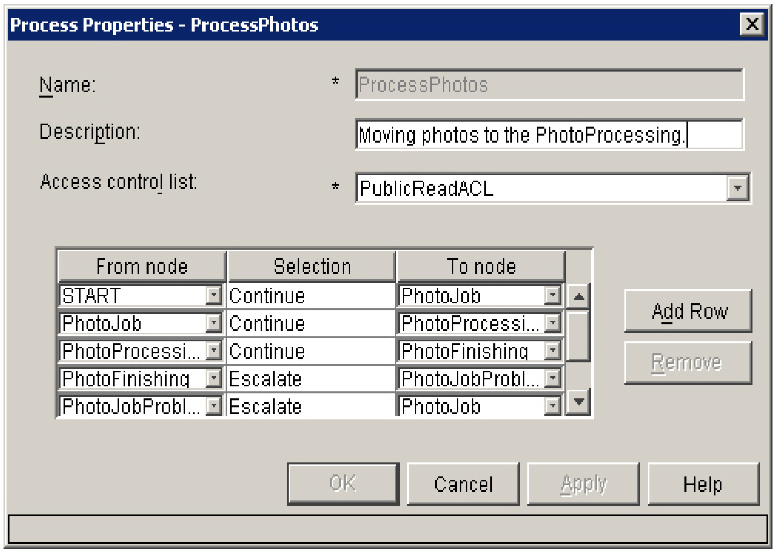
Figure 7–9 *Process procedure linking work nodes*

1. ___ Highlight **Processes** and Select **New**.
2. ___ Type **ProcessPhotos** for the process name.
3. ___ For the description, type **Moving photos to the PhotoProcessing.**
4. ___ Set the access control to **PublicReadACL.**
5. ___ Use Table 7–8 to add and setup each row of the document process.

Table 7–8 *ProcessPhotos document process*

From Node	Selection	To Node
Start	Continue	PhotoJob
PhotoJob	Continue	PhotoProcessing
PhotoProcessing	Continue	PhotoFinishing
PhotoProcessing	Escalate	PhotoJobProblem
PhotoJobProblem	Continue	PhotoFinishing
PhotoJobProblem	Escalate	PhotoJob
PhotoFinishing	Continue	End

6. ___ The *ProcessPhotos* process should resemble Figure 7–10.



Process Properties - ProcessPhotos

Name: * ProcessPhotos

Description: Moving photos to the PhotoProcessing.

Access control list: * PublicReadACL

From node	Selection	To node
START	Continue	PhotoJob
PhotoJob	Continue	PhotoProcessi...
PhotoProcessi...	Continue	PhotoFinishing
PhotoFinishing	Escalate	PhotoJobProbl...
PhotoJobProbl...	Escalate	PhotoJob

Figure 7–10 *ProcessedPhotos document process*

In order to demonstrate some of the document routing features it would be beneficial to have another document routing process. This will provide support for switching documents between processes.

7. ___ Highlight **Processes** and Select **New** to create a second process.

8. ___ Type **ProblemPhotoJobs** for the process name.

9. ___ For the description, type **Handling problem photos.**

10. ___ Set the access control to **PublicReadACL.**

11. ___ Now use Table 7–9 to setup a second document routing process.

Table 7–9 *ProblemPhotoJobs document process*

From Node	Selection	To Node
Start	Continue	PhotoJobProblems
PhotoJobProblems	Continue	PhotoJob
PhotoJobProblems	Escalate	END

Table 7–9 *ProblemPhotoJobs document process*

From Node	Selection	To Node
PhotoJob	Continue	PhotoFinishing
PhotoFinishing	Continue	End

Document Routing Example

With both processes defined, Figure 7–11 provides an example of the document flow for the photo jobs document routing process.

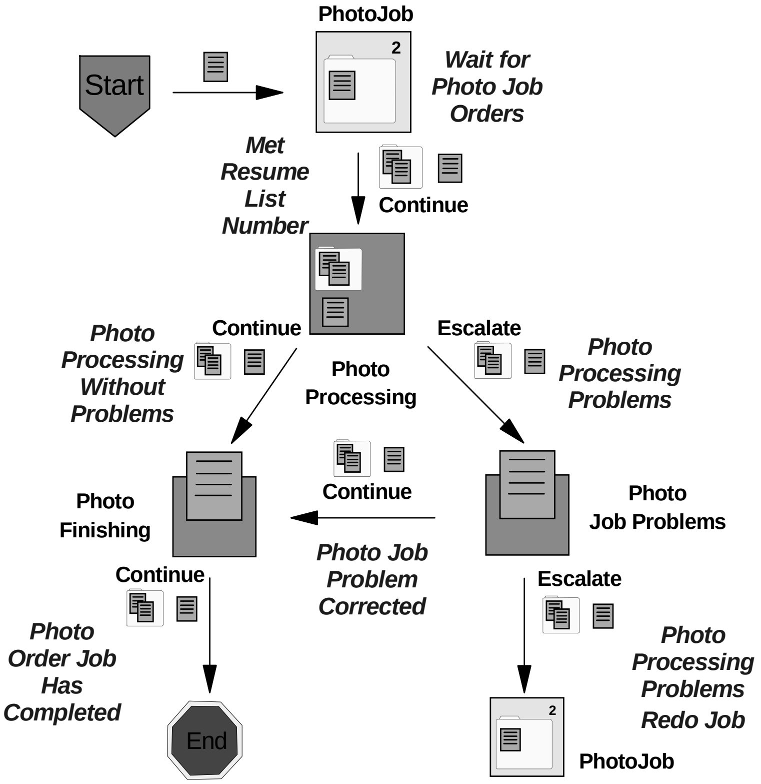

PhotoJob
2
Start
Wait for Photo Job Orders
Met Resume List Number
Continue
Photo Processing Without Problems
Continue
Escalate
Photo Processing
Photo Processing Problems
Continue
Photo Finishing
Photo Job Problems
Continue
Photo Job Problem Corrected
Escalate
Photo Order Job Has Completed
Photo Processing Problems Redo Job
End
2
PhotoJob

Figure 7–11 *Photo jobs document routing process*

In Figure 7–11 the *PhotoJob* collection work node is the first place documents or folders go when started on a document routing process. Documents imported into Content Manager and started on a document process at import time flow directly through the collection onto the next work node. Folders started on the process where the folder item type has not been included in the collection resume list also flow directly through the collection work node to the next work node. Only folders started on the process where the folder item type is defined in the collection work node resume list will be held in the collection point until the stated number of items have been added. Once the required number has been met the folder proceeds to the next work node. Items added to the folder continue to reside in the folder throughout the process.

In the above example, a folder with a defined resume list requiring two documents is started on the process with one contained item. The folder will be held until a second item is added to the folder. If a document is added directly to the process it flows directly to the work node named PhotoProcessing. When the second item is added (meeting the resume list required number of items) to the folder, the folder also continues to the PhotoProcessing work node.

Within PhotoProcessing, the user works with the documents individually started on the process or with the folder started on the process taking one of three actions: continue, escalate, or start on another document routing process (not depicted in Figure 7–11). If photoprocessing for the item (Order) is successful then ***continue*** moves the work package representing the individual document or folder to the next workbasket work node PhotoFinishing. If there is a problem with the photo processing for an order (item), the user ***escalates*** the job moving the document or folder represented by the work package to PhotoJobProblems. Within the PhotoJobProblem workbasket work node, if the problem has been corrected the user ***continues*** the document or folder on to the next work node PhotoFinishing. If a problem persists, the user ***escalates*** the document or folder which forces it to flow back through the PhotoJob process. At this point there should be other actions taken, but for demonstration purposes, this simple scenario will allow for pointing out how the clients handle document routing.

Notice that as the above document routing process has been defined, there has been no mention of Enterprise Information Portal Advanced WorkFlow. Each part of the document routing process is defined and contained in the Library Server database. For basic workflow needs, document routing should handle many of the scenarios needed for routing documents to different users. If full decision points and automated branching is needed, then the Enterprise Information Portal Advanced WorkFlow will need to be used.

Summary

This section has attempted to explain the document routing support added to Content Manager Version 8.1. The purpose of document routing is to provide a basic workflow process for handling the documents, images, and other files added to Content Manager, without the overhead of requiring a full workflow product. The *IBM Certification Solutions Expert (CSE) - IBM Content Manager Version 8 Certification Exam 442* covers the document routing added to Content Manager Version 8.1 and does not contain detailed implementation questions concerning the Advanced WorkFlow in Enterprise Information Portal. It is important to understand the distinctions between how the Content Manager document routing can solve solution problems versus the business process requirements that Enterprise Information Portal Advanced Workflow can handle. For example, the Content Manager document routing process is not intended to handle complex business processes requiring automated decision points base on some defined criteria within the process step.

Now that the fundamentals for setting up a document routing process have been covered, the remaining capabilities of document routing will be covered in the *Using Document Routing* sections of the *Client for Windows* and *eClient*, chapters.

CHAPTER 8

LDAP Integration

- IBM Directory Server
- Creating LDAP Entries
- Enabling LDAP
- Importing Users

In this chapter, you will be introduced to the Lightweight Directory Access Protocol (LDAP) enablement feature of Content Manager for Multiplatforms version 8.1. The IBM$^{(R)}$ Directory Server Version 4.1 will be used to install and populate an LDAP directory with user names. Steps will then guide you through enabling Content Manager for LDAP integration. Once done, user definitions in LDAP will be imported into Content Manager. This section is not intended to be a detail discussion on LDAP and the many options that it provides. The focus will be on the support Content Manager provides for LDAP.

Overview

The Content Manager LDAP enablement feature provides the support needed to have user IDs and passwords managed at the enterprise level in an LDAP directory. Content Manager will import and use the user definitions to populate Content Manager user profiles reducing the need to define user names and passwords directly in Content Manager. Doing this allows users to use the single sign-on user ID they may be using for Content Manager to also access other applications within their working environments.

Content Manager has been tested and supports importing of users and user authentication from the following LDAP enabled sources:

- *IBM Directory Server*. IBM Directory Server is a cross-platform, highly scalable, robust directory server included with the Content Manager package.
- *Windows 2000 Active Directory*. Active Directory is the name of the LDAP directory used by Microsoft ® for Windows 2000.
- *Lotus Domino Directory Notes ™ Address Book (NAB)*. Beginning with its Release 4.6, Lotus Domino also incorporates an LDAP service that allows LDAP clients to access the information stored in the Notes address book.

With the LDAP feature enabled for Content Manager, user IDs and passwords are authenticated against the LDAP defined entries when users sign-on Content Manager. Once verified, the user is granted access to the system and the privilege set defined for the user in the Content Manager user profile defines the maximum rights the user has once logged on. Aside from the user ID and password, the other information defined in LDAP for the user does not affect what they can do once signed onto Content Manager.

Content Manager provides two ways to import LDAP user definitions into Content Manager. The first is through the Content Manager New User profile definition. Support is provided to search an LDAP directory to locate a user to complete the user profile. Second, Content Manager provides an import utility that will batch import user definitions into Content Manager.

The Content Manager LDAP enablement feature can be enabled during Content Manager installation or after Content Manager has been installed. This guide will provide the steps for enabling LDAP after a Content Manager installation. For more information on enabling Content Manager LDAP, refer to *Planning and Installing Your Content Management System (GC27-1332)*.

Install IBM Directory Server

The steps in this section will guide you through setting up the IBM(R) Directory Server Version 4.1 on a Windows platform. IBM Directory Server is not covered on the *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* exam. What is covered on the exam are the Content Manager LDAP integration points. If you already have an LDAP installation populated with organizational information then proceed to the section of this chapter covering the steps required to enable Content Manager for LDAP. The following steps provide the minimal steps and information for just installing Directory Server.

8.1

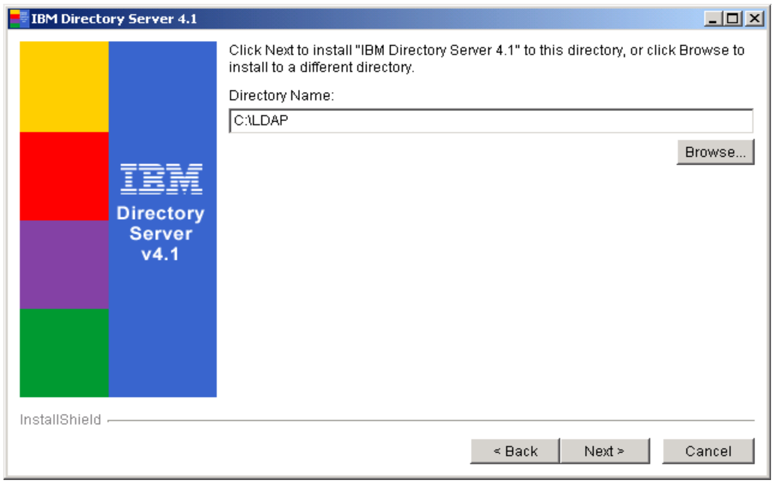
Note: Just for install, make sure there is an operating system user ID named db2admin with the password set to db2admin. If this is not done the Directory Server will not install correctly for the remaining steps involving Content Manager integration. The password can be reset after the Directory Server installation.

1. ___ Start **x:\WIN\IBMDirectory_WIN\ismp\setup.exe**.

   This assumes you are using the distribution media shipped with Content Manager Version 8.1.

2. ___ Select **English** as the language to be used.
3. ___ Select **OK**.
4. ___ Select **Next** on the Welcome Screen.
5. ___ **Accept** the license agreement and select **Next**.
6. ___ Select **Next** on the *The following applications have been identified* screen
7. ___ Type **C:\LDAP** as the **Directory Name**, **(**see Figure 8–1 on page 236).
8. ___ Select **Next**.
9. ___ Select **English** on the *Select language for IBM Directory* screen.
10. ___ Select **Next**.

.



Click Next to install "IBM Directory Server 4.1" to this directory, or click Browse to install to a different directory.

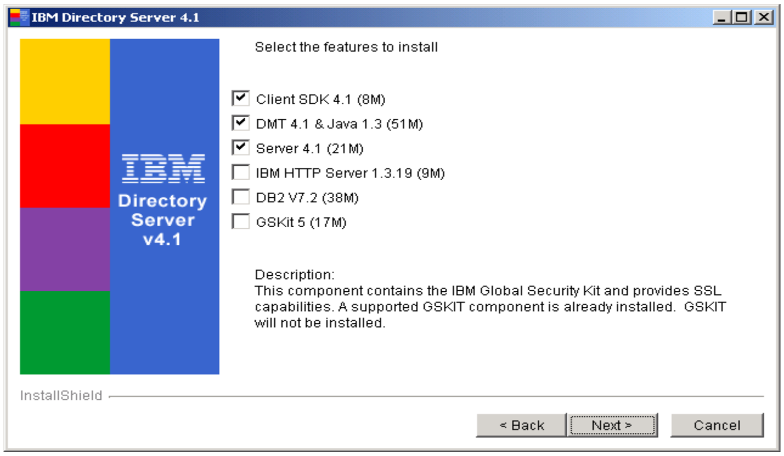
Directory Name:

C:\LDAP

Figure 8–1 *Directory Server installation destination*

11. ___ Select **Custom** on the *Choose the setup type that best meets your needs* screen.

12. ___ Take the defaults of Client SDK, DMT 4.1, and Server 4.1, (see Figure 8–2).



Select the features to install

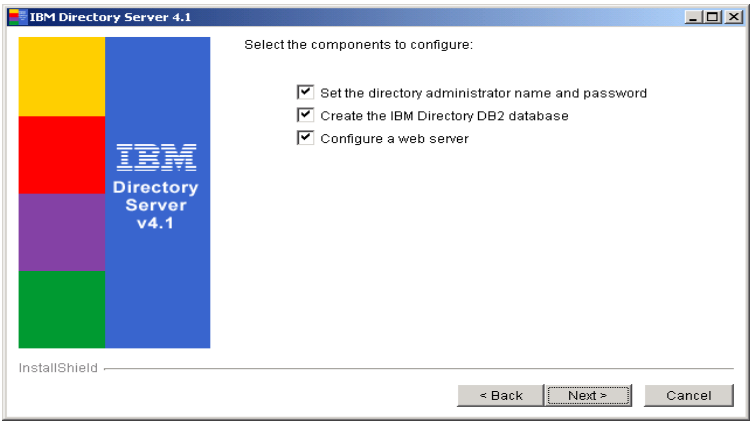
☑ Client SDK 4.1 (8M)
☑ DMT 4.1 & Java 1.3 (51M)
☑ Server 4.1 (21M)
□ IBM HTTP Server 1.3.19 (9M)
□ DB2 V7.2 (38M)
□ GSKit 5 (17M)

Description:
This component contains the IBM Global Security Kit and provides SSL capabilities. A supported GSKIT component is already installed. GSKIT will not be installed.

Figure 8–2 *Default features to install for Directory Server*

13. ___ Select **Next**.

14. ___ Select all the options on the *Select the components to configure* screen, (see Figure 8–3).



Select the components to configure:

☑ Set the directory administrator name and password

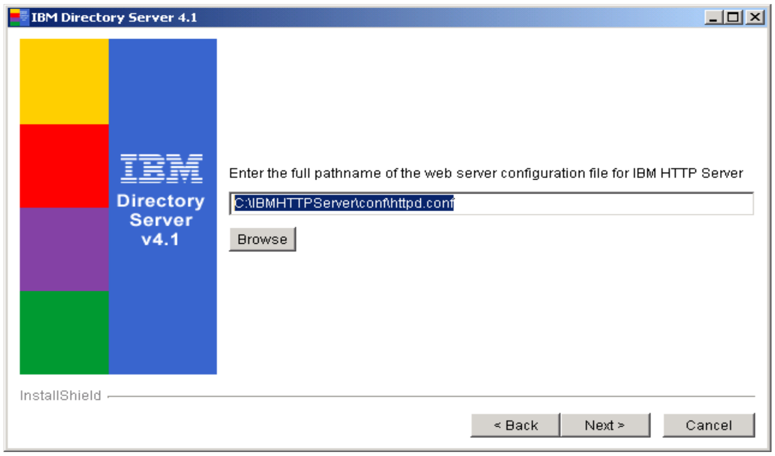
☑ Create the IBM Directory DB2 database

☑ Configure a web server

Figure 8–3 *Directory Server components to configure*

15. ___ Select **Next**.

16. ___ Select **C:\IBM HTTP Server\conf\httpd.conf** as the default web server. This should be the location of the HTTP server if you followed the defaults during installing the prerequisites earlier in this guide, (see Figure 8–4).



Enter the full pathname of the web server configuration file for IBM HTTP Server

C:\IBMHTTPServer\conf\httpd.conf

Figure 8–4 *Enter IBM HTTP server configuration file*

17. ___ Select **Next**.

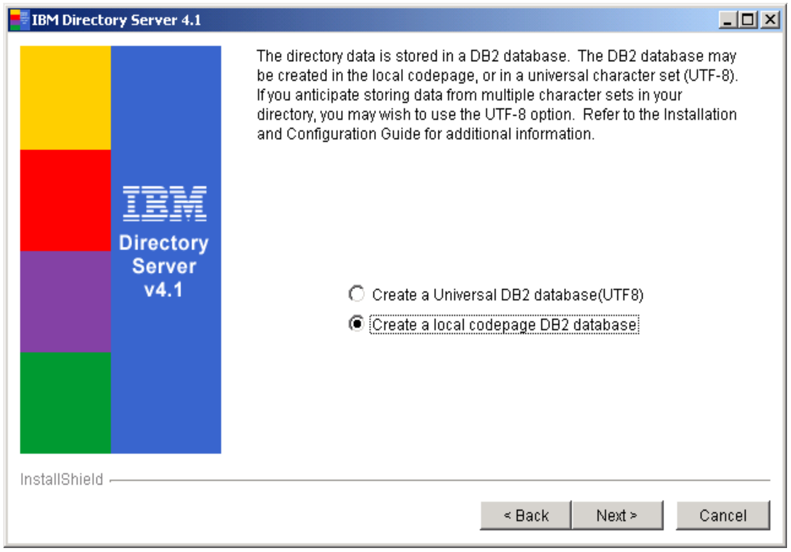
18. ___ Use Table 8–1 to complete the fields on the *Enter a new LDAP administrator Distinguished Name and Password*. The distinguished administrator name and password will be needed on the Content Manager LDAP integration screens.

Table 8–1 *Directory Server LDAP name and password*

Field	Value
Administrator distinguished name	cn=root
Administrator password	password

19. ___ Select **Next**.

20. ___ Select **Create a local codepage DB2 database**, (see Figure 8–5).



The directory data is stored in a DB2 database. The DB2 database may be created in the local codepage, or in a universal character set (UTF-8). If you anticipate storing data from multiple character sets in your directory, you may wish to use the UTF-8 option. Refer to the Installation and Configuration Guide for additional information.

○ Create a Universal DB2 database(UTF8)

● Create a local codepage DB2 database

Figure 8–5 *Create a local codepage DB2 database*

21. ___ Select **Next**.

22. ___ Select **C:** for the directory drive and then **Next**.

23. ___ On the setting confirmation panel, verify the settings, and select **Next**.

24. ___ On the *Please read the information below* screen select **Next**.

25. ___ Select **Next** again.

26. ___ Select **Yes, restart my system**, and select **Next**.

27. ___ Select **Finish** to complete the installation and re-boot the system.

When the server starts up, the c:\LDAP\bin\ldapcfg.exe program will run to setup LDAP. Do not close this window or the LDAP integration will fail. The setup program will create the LDAP Administrator user ID and assign the required rights. This may take a while so let it run. If after a period of time the process has not ended and you do not see additional configuration lines being displayed for the command window running ldapcfg, the process may be hung. If this is the case, then repeat the LDAP installation.

After installation has completed, additional LDAP configuration will be needed before it can be used for Content Manager.

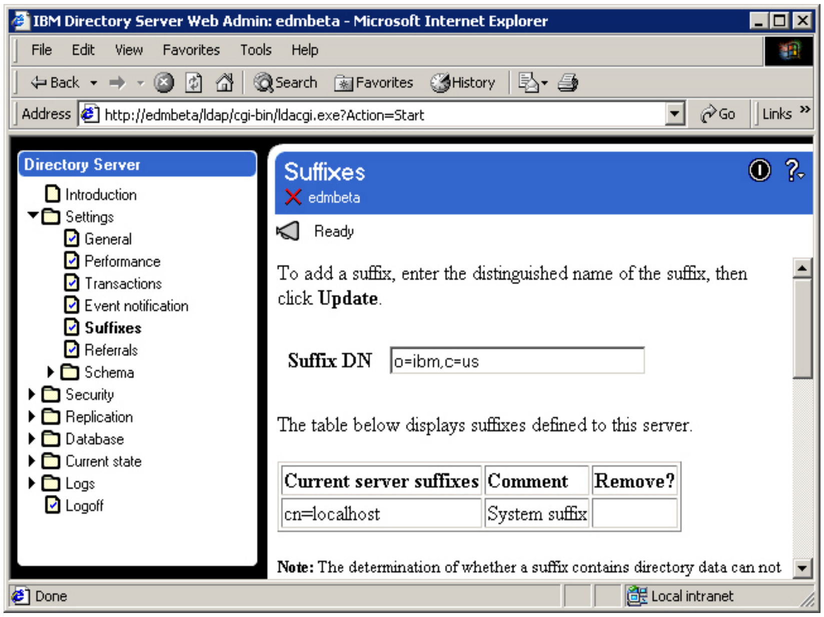
Configure IBM Directory Server

This section will provide the steps to configure the IBM Directory server on a Windows platform. The intent of this study guide is to only cover the required steps to configure the IBM Directory Server to the point where the Content Manager LDAP enablement feature can be demonstrated. Therefore, minimal information on the IBM Directory Server will be provided beyond configuration.

1. ___ Select **Services**.
2. ___ Stop the **IBM HTTP Administration** service.
3. ___ Stop the **IBM HTTP Server** service.
4. ___ Restart the **IBM HTTP Server** service.
5. ___ Restart the **IBM HTTP Administration** service.

   Doing the above activates the LDAP changes made for the web server.
6. ___ Open an **Internet Explorer** browser window.
7. ___ Type **http://hostname/ldap/** as the URL to start the Directory Server Administration window. The **hostname** should be the one for the machine being used for this exercise.
8. ___ Type **cn=root** for the Admin ID and **password** for password.
9. ___ Select **Logon**.
10. ___ Expand **Settings** on the left navigation bar.
11. ___ Select **Suffix** to display the suffixes screen.
12. ___ Type **o=IBM,c=us** as the **Suffix DN**, (see Figure 8–6).

    This sets the organizational unit to IBM and the country code to US.
13. ___ Select **Update**.



To add a suffix, enter the distinguished name of the suffix, then click **Update**.

Suffix DN o=ibm,c=us

The table below displays suffixes defined to this server.

Current server suffixes	Comment	Remove?
cn=localhost	System suffix	

Note: The determination of whether a suffix contains directory data can not

Figure 8–6 *Define the LDAP suffix for organization unit and country*

14. ___ Expand **Current state** on the left navigation bar.

15. ___ Select **Start/Stop** to stop the Directory Server.

16. ___ On the right side of the screen where it says **Start**. Select the **Start** button to restart the Directory Server. It may take a few minutes to start the LDAP server.

17. ___ Select **Logoff** on the left navigation bar.

18. ___ Select **Logoff**.

19. ___ Close the browser. The initial configuration has been completed.

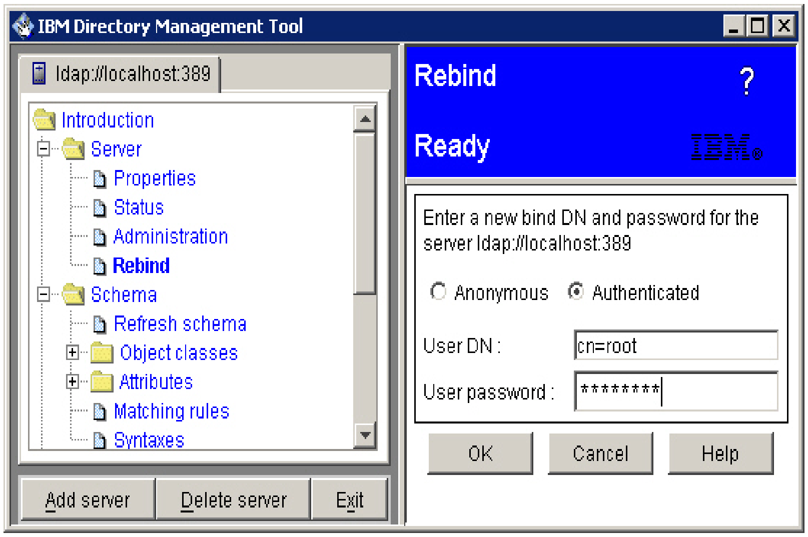
Add Organizational Information

The steps in this section will add user information to the LDAP database instance of the Directory Server. This information will later be used to import users into Content Manager. If you already have an LDAP installation populated with organizational information then proceed to the section of this chapter covering the steps required to enable Content Manager for LDAP.

1. ___ Start the **Directory Management Tool**.

(**Start** | **Programs** | **IBM Directory Server 4.1** | **Directory Management Tool**)

2. ___ Expand **Server** on the left navigation bar, (see Figure 8–7).



Enter a new bind DN and password for the server ldap://localhost:389

○ Anonymous ● Authenticated

User DN : cn=root

User password : ********

Figure 8–7 *Directory server rebind using domain name*

3. ___ Select **Rebind**.

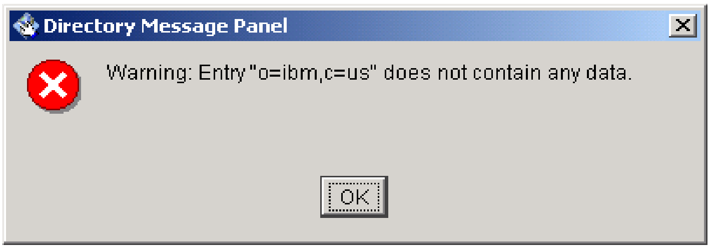
4. ___ Select the **Authenticated** radio button.

5. ___ Type **cn=root** as the *User DN* (User Domain Name).

6. ___ Type **password** as the *User password*.

7. ___ Select **OK**.

8. ___ If displayed, ignore the error message shown in Figure 8–8.



Warning: Entry "o=ibm,c=us" does not contain any data.

Figure 8–8 *Warning indicating data has not been added to LDAP*

9. ___ The *Browse tree* screen should now be presented, (see Figure 8–9).

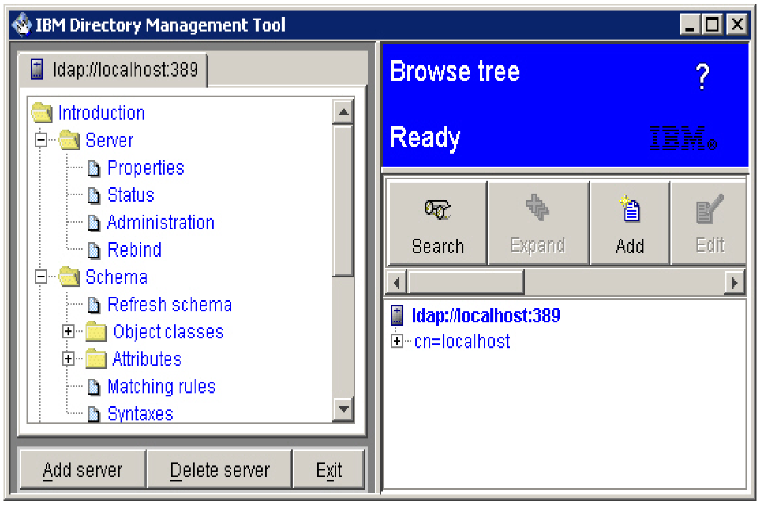
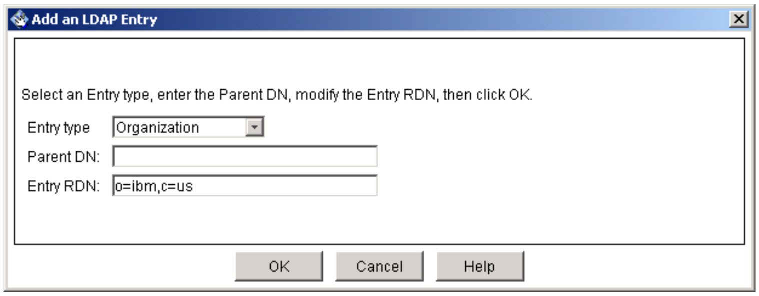


Figure 8–9 *Directory browse tree screen*

10. ___ Highlight **ldap://localhost:389** and select **Add** on the toolbar.

11. ___ This will display the *Add an LDAP Entry* screen, (see Figure 8–10 on page 244).



Add an LDAP Entry

Select an Entry type, enter the Parent DN, modify the Entry RDN, then click OK.

Entry type: Organization

Parent DN:

Entry RDN: o=ibm,c=us

Figure 8–10 *Screen for adding LDAP entries*

12. ___ Use Table 8–2 for adding an LDAP organizational unit entry.

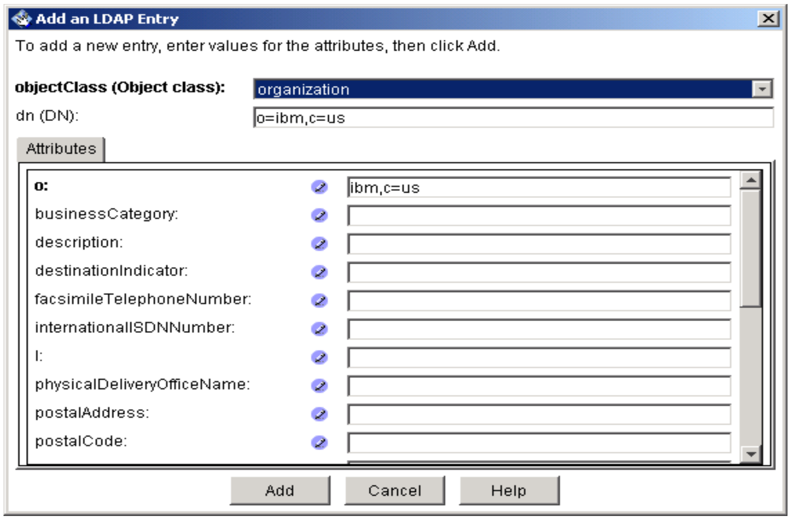
Table 8–2 *Values for adding LDAP entries*

Field	Value
Entry type	Organization
Parent DN	
Entry RDN	o=ibm,c=us

13. ___ Select **OK** to display the *Add an LDAP Entry* attributes screen,

14. ___ Type **ibm,c=us** as the value for the **o:** attribute, (see Figure 8–11).

15. ___ Select **Add** to return to the browse screen.



Add an LDAP Entry

To add a new entry, enter values for the attributes, then click Add.

objectClass (Object class): organization

dn (DN): o=ibm,c=us

Attributes	
o:	ibm,c=us
businessCategory:	
description:	
destinationIndicator:	
facsimileTelephoneNumber:	
internationalISDNNumber:	
l:	
physicalDeliveryOfficeName:	
postalAddress:	
postalCode:	

Figure 8–11 *Add an LDAP entry attribute*

16. ___ Highlight **o=ibm,c=us** on the Browse tree.

17. ___ Select **Add** from the toolbar.

18. ___ Use Table 8–3 to add an organizational unit LDAP entry.

Table 8–3 *Values for adding an organizational unit*

Field	Value
Entry type	Organizational unit
Parent DN	o=ibm,c=us
Entry RDN	ou=accounting

19. ___ Select **OK**.

20. ___ Type **accounting** for the organizational unit **ou:** attribute.

21. ___ Select **Add**.

22. ___ Expand **o=ibm,c=us** on the Browse tree.

23. ___ Highlight **ou=accounting** on the Browse tree.

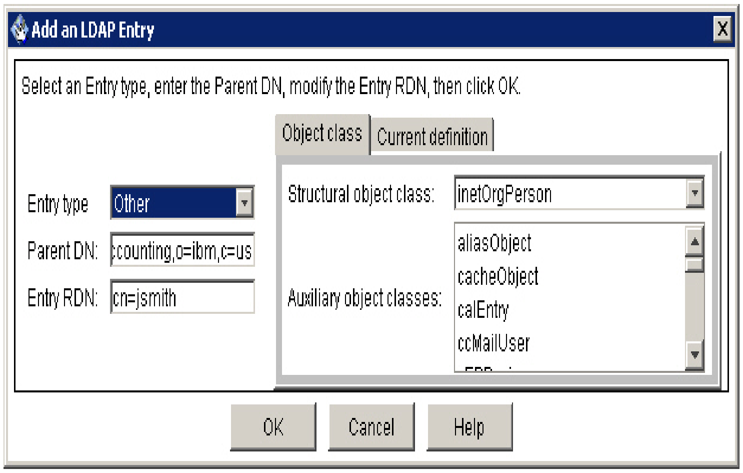
24. ___ Select **Add** from the toolbar.

25. ___ Use Table 8–4 to add another LDAP entry**.**

Table 8–4 *Attribute values the organizational unit*

Attribute Field	Value
Entry type	Other
Parent DN	ou=accounting,o=ibm,c=us
Entry RDN	cn=jsmith
Structural Object Class	inetOrgPerson

26. ___ The screen should resemble Figure 8–12.



Add an LDAP Entry

Select an Entry type, enter the Parent DN, modify the Entry RDN, then click OK.

Entry type: Other

Parent DN: :counting,o=ibm,c=us

Entry RDN: cn=jsmith

Structural object class: inetOrgPerson

Auxiliary object classes:
aliasObject
cacheObject
calEntry
ccMailUser

Figure 8–12 *Adding an organization person unit*

27. ___ Select **OK**.

28. ___ Use Table 8–5 the organization person unit attribute values.

Table 8–5 *The organization person unit attribute values*

Attribute Field	Value
cn (Common name)	jsmith
sn (Last Name)	Smith

Table 8–5 *The organization person unit attribute values*

Attribute Field	Value
uid	jsmith
userPassword	password

29. ___ Select **Add**.

30. ___ Expand **o=ibm,c=us** on the Browse tree.

31. ___ Highlight **ou=accounting** on the Browse tree and use Table 8–6 and Table 8–7 to create another person record.

Table 8–6 *Values for a second person record*

Attribute Field	Value
Entry type	Other
Parent DN	ou=accounting,o=ibm,c=us
Entry RDN	cn=user1
Structural Object Class	inetOrgPerson

32. ___ Select **OK**

Table 8–7 *Attribute values for the second person record*

Attribute Field	Value
cn (Common name)	user1
sn (Last Name)	General
uid	user1
userPassword	password

33. ___ Select **Add**.

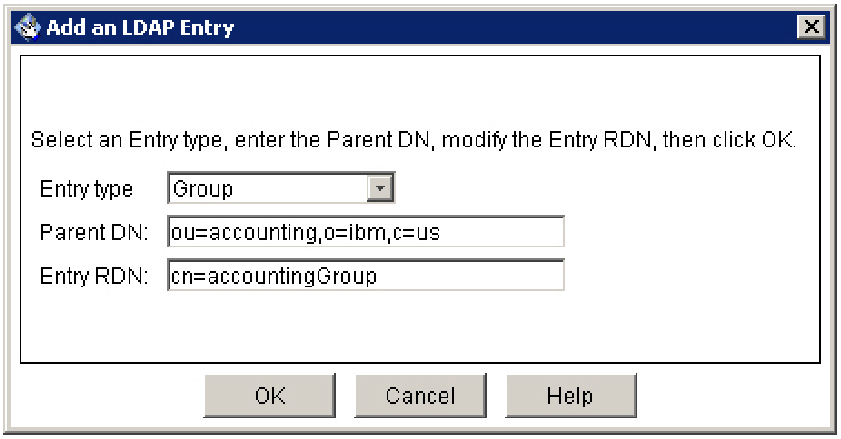
Now you need to add a group in order to complete the Content Manager integration.

34. ___ Select **ldap://localhost:389**.

35. ___ Select **o=ibm,c=us**.

36. ___ Select **ou=accounting**.

37. ___ Select **Add from the tool bar** to display the *Add an LDAP Entry* screen in Figure 8–13.



Select an Entry type, enter the Parent DN, modify the Entry RDN, then click OK.

Entry type: Group

Parent DN: ou=accounting,o=ibm,c=us

Entry RDN: cn=accountingGroup

Figure 8–13 *LDAP add a group entry*

38. ___ Select **Group** as the *Entry Type.*

39. ___ Type **ou=accounting,o=ibm,c=us** as the **Parent DN**.

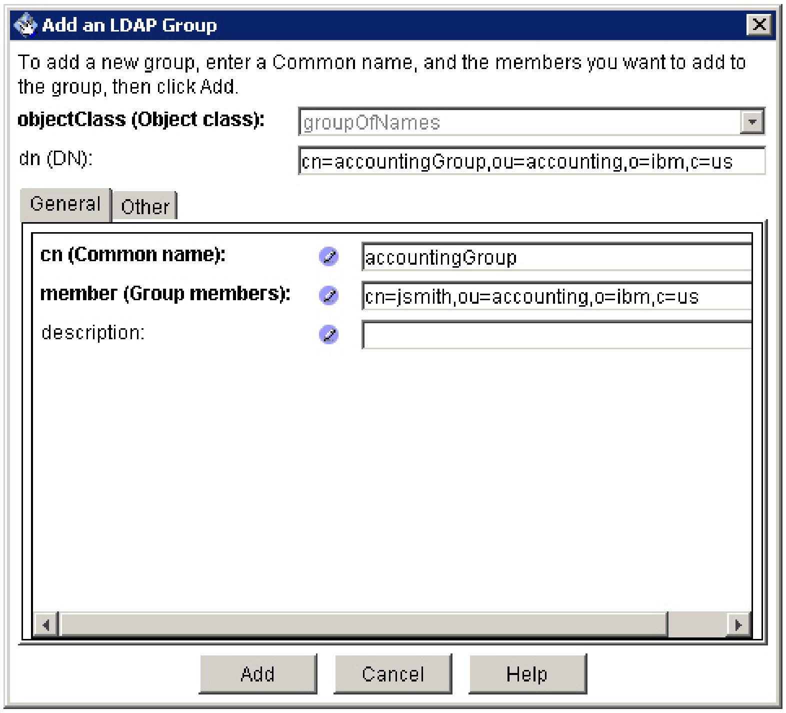
40. ___ Type **cn=accountingGroup** as the **Entry RDN**.

41. ___ Select **OK**.

42. ___ The *Add an LDAP Group* screen will be displayed, see figure

43. ___ Type **cn=jsmith,ou=accounting,o=ibm,c=us** as the member name.

44. ___ Notice the Object Class name of **groupOfNames**. This will be needed on the Content Manager LDAP import utility screen defined later, along with the group name.



Add an LDAP Group

To add a new group, enter a Common name, and the members you want to add to the group, then click Add.

objectClass (Object class): groupOfNames

dn (DN): cn=accountingGroup,ou=accounting,o=ibm,c=us

cn (Common name): accountingGroup

member (Group members): cn=jsmith,ou=accounting,o=ibm,c=us

description:

Figure 8–14 *Add an LDAP Group*

45. ___ Select **Add** to add the group.

Now that two person units and a group have been added to LDAP, the Content Manager integration can be completed. Use the above steps to add more users if you desire a larger sample for integration (see Figure 8–14).

Enable Content Manager LDAP Integration

To enable LDAP in Content Manager the properties file has to be generated. Once generated the properties file needs to be installed on both the Library Server and Resource Manager. Then the user exit used for LDAP integration needs to be installed. Some additional Directory Server applications will need to be installed and configured. Then the Secured Sockets Layer (SSL) will have to be configured for LDAP server communication.

Generate the Properties File

1. ___ Start the Content Manager System Administration Client.
2. ___ Logon using **icmadmin** and **password**.
3. ___ Select the **Tools** menu and then **LDAP Configuration**.
4. ___ Select **Enable LDAP User import and authentication**.
5. ___ Select the **LDAP Configuration Server** tab and use Table 8–8 to complete the options on the screen.

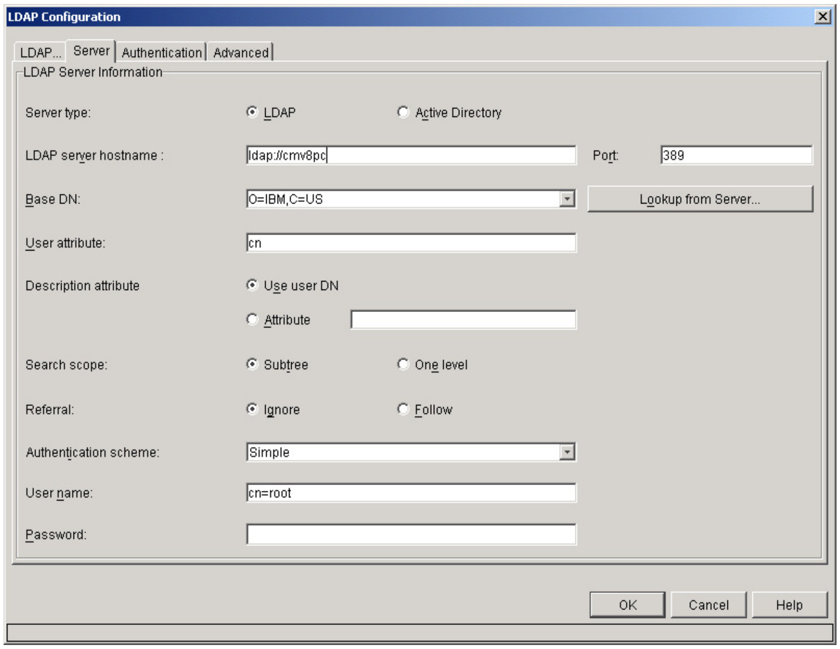
Table 8–8 *Content Manager LDAP server information options*

Option	Value to be selected
Server Type	LDAP
LDAP server hostname	Hostname of your machine. Use **cmv8pc** if following the examples in this book.
Port	389
Base DN:	Select the **Lookup from Server** button and choose **O=IBM,C=US**.
User Attribute	uid
Description Attribute	Select **Use user DN**.
Search Scope	Select **Subtree**
Referral	Ignore
Authentication Schema	Simple

Table 8–8 *Content Manager LDAP server information options*

Option	Value to be selected
User name	cn=root
Password	password

6. ___ The *LDAP Configuration* screen should look like Figure 8–15.



Server type: ● LDAP ○ Active Directory

LDAP server hostname : ldap://cmv8pc Port: 389

Base DN: O=IBM,C=US

User attribute: cn

Description attribute ● Use user DN ○ Attribute

Search scope: ● Subtree ○ One level

Referral: ● Ignore ○ Follow

Authentication scheme: Simple

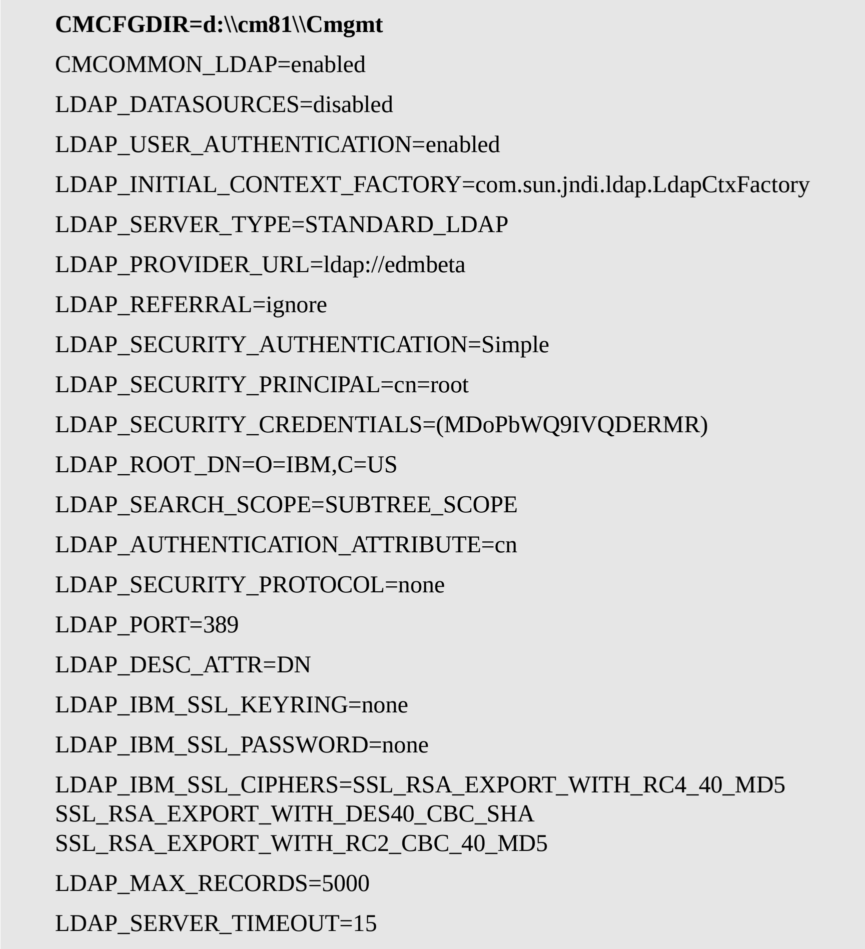
User name: cn=root

Password:

Figure 8–15 *Content Manager LDAP server information*

7. ___ Select **OK**.

When the configuration is complete, a ***cmbcmenv.properties*** file (see Figure 8–16 on page 252) is generated in the directory pointed to by the *CMCOMMON* environment variable on the system where the Content Manager System Administration Client is being run. If this in on the Content Manager server, the file will be placed in the common directory, by default x:\Program Files\IBM\Cmgmt. If the above process was completed using the System Administration Client on a remote workstation, then the ***cmbcmenv.properties*** file has been stored in the Content Manager common directory on the remote workstation. In order for LDAP to work with the Library Server and Resource Manager the file needs to be copied to each of the servers. When copied, make sure the CMCFGDIR=x:\\cm81\cmgmt line is updated for the location of the common files on the server where the file is being copied.



```
CMCFGDIR=d:\\cm81\\Cmgmt
CMCOMMON_LDAP=enabled
LDAP_DATASOURCES=disabled
LDAP_USER_AUTHENTICATION=enabled
LDAP_INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
LDAP_SERVER_TYPE=STANDARD_LDAP
LDAP_PROVIDER_URL=ldap://edmbeta
LDAP_REFERRAL=ignore
LDAP_SECURITY_AUTHENTICATION=Simple
LDAP_SECURITY_PRINCIPAL=cn=root
LDAP_SECURITY_CREDENTIALS=(MDoPbWQ9IVQDERMR)
LDAP_ROOT_DN=O=IBM,C=US
LDAP_SEARCH_SCOPE=SUBTREE_SCOPE
LDAP_AUTHENTICATION_ATTRIBUTE=cn
LDAP_SECURITY_PROTOCOL=none
LDAP_PORT=389
LDAP_DESC_ATTR=DN
LDAP_IBM_SSL_KEYRING=none
LDAP_IBM_SSL_PASSWORD=none
LDAP_IBM_SSL_CIPHERS=SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
LDAP_MAX_RECORDS=5000
LDAP_SERVER_TIMEOUT=15
```

Figure 8–16 *Sample cmbcmenv.properties file*

Note: When modifying LDAP settings try to always use the System Administration Client LDAP configuration support in order to avoid corrupting the *cmbcmenv.properties* file.

Install the Properties File

The file *cmbcmenv.properties* is used by the Content Manager System Administration Client for importing users from the LDAP server, in this case the IBM Directory Server. The Library Server and Resource Manager also require this file for user authentication against the information stored in the LDAP server. If LDAP was configured using a remote System Administration Client, then the file will need to be copied to both the Library Server and Resource Manager.

Installing the Properties File on the Library Server

The following only needs to be done if the LDAP integration was setup using a System Administration Client that was not on the Library Server machine. If so, copy the *cmbcmenv.properties* file from the remote System Administration Client machine CMCOMMON directory (type set CMCOMMON on a Windows command line for the directory name) to the *CMCOMMON* directory on the Library Server machine. If there are multiple library server databases installed on the machine, copy the file into the *CMCOMMON* directory with the same name as the Library Server database name.

The Library Server LDAP user-exit looks for the *cmbcmenv.properties* in a file system directory named the same as the referenced Library Server database. This default would be *%CMCOMMON%/ICMNLSDB* on a Windows machine where CMCOMMON pointed to \Program Files\IBM\Cmgmt. If the properties file cannot be found in a directory matching the Library Server database the Library Server looks for the file in the *CMCOMMON* referenced directory.

For the purposes of this exercise, leave the file in the %CMCOMMON% referenced directory.

Installing the Properties File on the Resource Manager

Like the Library Server, the Resource Manager needs the *cmbcmenv.properties* file to authenticate users access resources on the Resource Manager. Even if the System Administration Client was run from the same machine as the Resource Manager, the file needs to be copied into the Resource Manager WebSphere directory.

1. ___ Copy the *cmbcmenv.properties* file from the %CMCOMMON% directory (IBM\cmgmt) to the Resource Manager application directory under Websphere *<WAS_HOME>\installedApps\icmrm.ear\icmrm.war\WEB-INF\classes\com\ibm\mm\icmrm*.

Where ***icmrm*** is the resource manager default application name.

2. ___ Edit the *cmbcmenv.properties* file in the above directory.
3. ___ Change all the encrypted passwords to clear text passwords. When you restart the server, the passwords will be re-encrypted.

   For example, in Figure 8–16 on page 252 change **MDoPbWQ9IVQDERMR** on the following line to password:
   LDAP_SECURITY_CREDENTIALS=(MDoPbWQ9IVQDERMR)
4. ___ Restart the server.

8.1

> **Note:** The change password request in the LDAP server is not supported. You must use the LDAP servers administrative tools to change the password. For example, use the IBM Directory Server Management Tool to change the password used for Directory Server.

Install the User Exit

The user exit file (*ICMXLSLG.DLL)* needed for LDAP integration is located in the *ldap* directory in the Content Manager installation directory (type **set icmroot** for the name of the root directory). This file has to be copied into the Library Server DLL directory representing the Library Server database for which you are connecting.

On a Windows Workstation

Copy the *ICMXLSLG.DLL LDAP* user-exit DLL file from the *%ICMROOT%\LDAP* directory into the *%ICMROOT%\<DBNAME>\DLL* directory. The <*DBNAME*> represents your Library Server database name.

On a UNIX Workstation

1. ___ Copy the *ICMXLSLG.DLL LDAP* user-exit DLL from the *%ICMROOT%/LDAP* directory into the *$ICMDLL/<DBNAME>/DLL* directory.

8.1

> **Note:** When copying the ICMXLSLG.DLL file, remember to preserve the uppercase characters in the name.

2. ___ On UNIX, set the permission on the copied DLL file.

For example, if the *<DBNAME>* is *ICMNLSDB*.

```
cd $ICMDLL
cd ICMNLSDB/DLL
cp $ICMROOT/ldap/ICMXLSLG.DLL.
chmod 555 ICMXLSLG.DLL
```

8.1

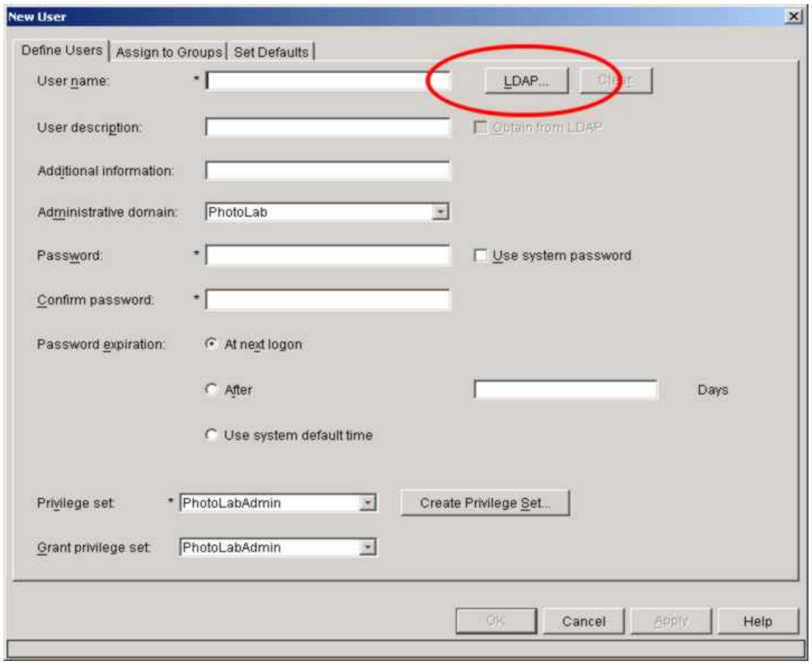
Note: Make sure that the *profile* for the *icmadmin* user and the */home/$DB2INSTANCE/sqllib/db2profile* have been updated for the *CMCOMMON* environment variable.

Import Users from LDAP server

With the IBM$^{(R)}$ Directory Server Version 4.1 installed and the Content Manager LDAP feature enabled it is now time to import users from LDAP into Content Manager. There are two ways to import user information from an LDAP server into the Content Manager system. The first is to use the Content Manager System Administration Client to create users. The new user definition screen contains an LDAP option for importing a user definition. The second method is to use the LDAP import utility provided with Content Manager. This would be beneficial for importing a large number of user definitions at one time.

Import Users using System Administration Client

1. ___ Start the **Content Manager System Administration Client**.
2. ___ Expand **Authentication**.
3. ___ Highlight **Users** and select **New**.



User name: *
User description:
☐ Obtain from LDAP
Additional information:
Administrative domain: PhotoLab
Password: *
☐ Use system password
Confirm password: *
Password expiration: ● At next logon
○ After Days
○ Use system default time
Privilege set: * PhotoLabAdmin
Grant privilege set: PhotoLabAdmin

Figure 8–17 *New user definition with LDAP option*

4. ___ The *New User* definition screen will be displayed.

5. ___ Notice the **LDAP** button, (see Figure 8–17).

6. ___ Select **LDAP** to import a user.

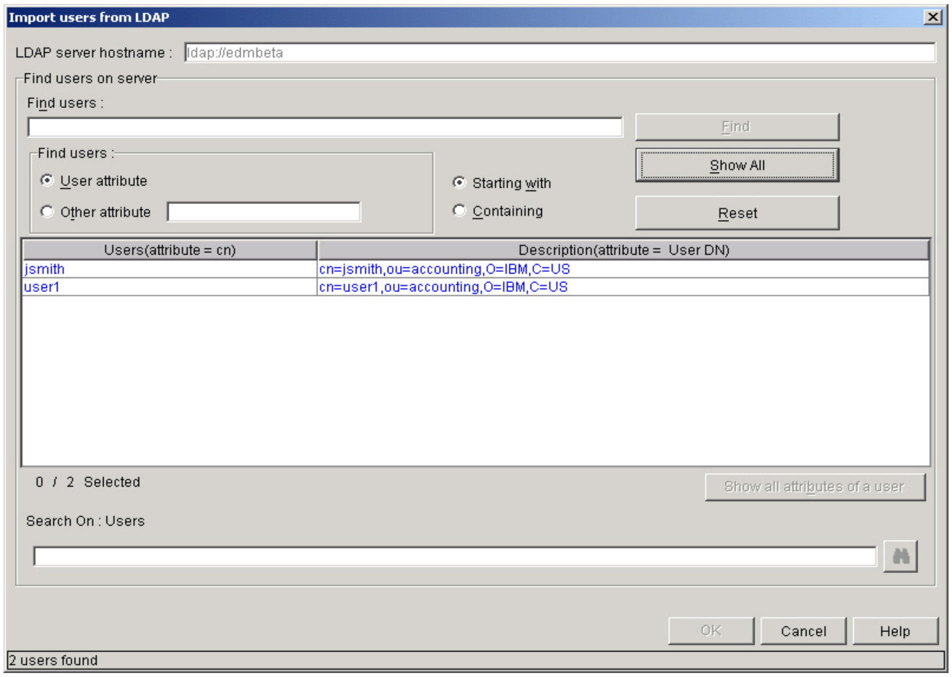
7. ___ The ***Import users from LDAP*** screen will be displayed.

8. ___ Select **Show ALL**.

9. ___ A warning message will be displayed concerning the maximum number of users on import limited to 5000.

10. ___ Select **Yes** to clear the warning message.

11. ___ Based on the preceding steps in this chapter, two user entries should be listed: jsmith and user1, (see Figure 8–18).



Import users from LDAP

LDAP server hostname : ldap://edmbeta

Find users on server

Find users :

Find users :

● User attribute

○ Other attribute

● Starting with

○ Containing

Users(attribute = cn)	Description(attribute = User DN)
jsmith	cn=jsmith,ou=accounting,O=IBM,C=US
user1	cn=user1,ou=accounting,O=IBM,C=US

0 / 2 Selected

Search On : Users

2 users found

Figure 8–18 *Import users from LDAP screen*

12. ___ Notice on the *Import users from LDAP* screen that you can search based on the user name or attributes.

13. ___ Highlight the ***jsmith*** entry in search hit list.

14. ___ Select **OK**.

15. ___ Notice on the Content Manager ***New User*** definition screen the user information and password options have been grayed. The information from LDAP will be used.

16. ___ To complete the user definition, assign jsmith to the **DefaultDomain** (if Administrative Domains have been installed) and take the remaining defaults.

17. ___ Select **OK** to save the new user definition for jsmith.

8.1

Note: The System Administraiton Client can only be used for importing a single LDAP user record.

Import Users Using the LDAP Import Utility

The LDAP User Import utility makes it easy for you to import groups and users defined in an LDAP directory into an IBM Content Manager for Multiplatforms (CM) database.

You can specify criteria to filter users you want to import and you can schedule periodic updates, therefore ensuring that users added to or deleted from the LDAP directory are also added to or deleted from the CM or EIP database. After importing groups of LDAP users, you can use the system administration client to modify user attributes according to the requirements of your Content Manager system (see Figure 8–19).

When invoked, the utility reads information about the LDAP server from the *cmbcmenv.properties* file.

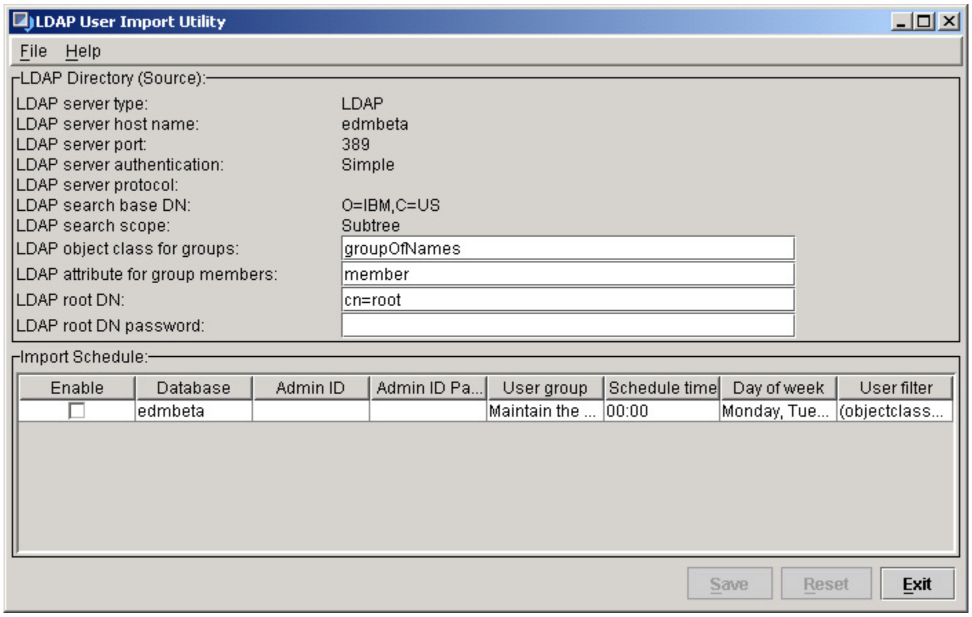
1. ___ Start the Content Manager **LDAP User Import Utility**.

   Start | **Programs** | **IBM Content Manager for Multiplatforms** | **LDAP User Import Scheduler**.

   Or run cmldapimptool81.bat from the %CMCOMMON%\ADMIN\COMMON directory.

2. ___ A screen similar to Figure 8–19 will be displayed listing the library server database that has been defined for your server.

   The information displayed in the *LDAP Directory (Source)* area is obtained from the `cmbcmenv.properties` file, (see Figure 8–16 on page 252). It shows the basic information concerning your LDAP server such as the host name, port number, authentication protocol, and search base distinguished name (DN). Some of this information is provided for review purposes only; you cannot change it.



LDAP Directory (Source):

LDAP server type: LDAP
LDAP server host name: edmbeta
LDAP server port: 389
LDAP server authentication: Simple
LDAP server protocol:
LDAP search base DN: O=IBM,C=US
LDAP search scope: Subtree
LDAP object class for groups: groupOfNames
LDAP attribute for group members: member
LDAP root DN: cn=root
LDAP root DN password:

Import Schedule:

Enable	Database	Admin ID	Admin ID Pa...	User group	Schedule time	Day of week	User filter
□	edmbeta			Maintain the ...	00:00	Monday, Tue...	(objectclass...

Figure 8–19 *LDAP user import utility*

3. ___ Review the LDAP object class for groups.

The groupOfNames object class was used to add the accountingGroup to your LDAP directory. It should be displayed so take the default.

4. ___ Review the LDAP attribute for group members attribute.

It needs to be **members** to match where the **cn=jsmith,ou=accounting,o=ibm,c=us** distinguished name entry was made when adding a group to LDAP.

5. ___ Make sure the LDAP Root DN is set to **cn=root**.

The Distinguished Name of the LDAP directory’s root user allows the LDAP User Import utility to access the directory and read or update information in it.

6. ___ Type **password** for the LDAP root DN password.

7. ___ Under Import Schedule, select **Enable** for the LDAP server defined in this chapter. The database name should be your Content Manager Library Server database name.

8. ___ Type **icmadmin** for the Admin ID and **password** for the Admin ID

Password. These are the defined administration IDs for the Library Server database.

9. ___ Select **User Group** to display the LDAP group policy import options shown in Figure 8–20.

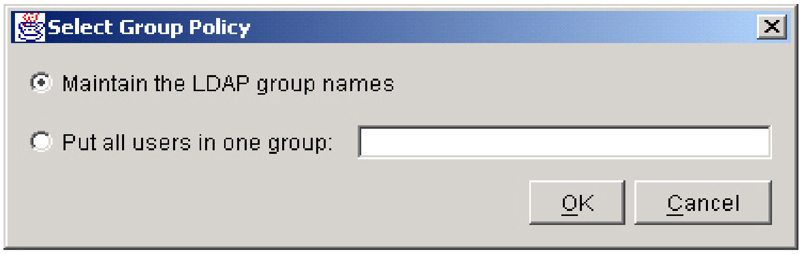

Select Group Policy
● Maintain the LDAP group names
○ Put all users in one group:
OK
Cancel

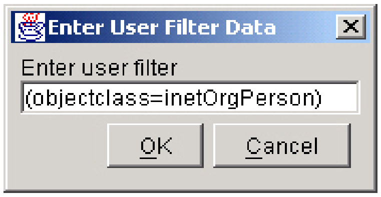
Figure 8–20 *LDAP group policy import options*

10. ___ Select **Maintain the LDAP group names**.

This uses information in the LDAP group object class and the LDAP attribute for group member's fields to import LDAP data maintaining the respective groups.

11. ___ Scheduled time is the time setting in 24:00 segments that the utility will run. Set the time shortly after your current time so you can see the results of the import.

12. ___ Select **User Filer** to specify the object class used for users in LDAP. This would be the *(objectclass=inetOrgPerson)* used to define our LDAP users.



Enter user filter (objectclass=inetOrgPerson)

Figure 8–21 *LDAP import utility user class*

13. ___ Type **(objectclass=inetOrgPerson)** on the user filter screen Figure 8–21.

When the import utility runs, groups and users that satisfy the filter criteria will be added to the Content Manager database if they do not already exist.

14. ___ Select **OK**.

15. ___ Select **Save**.

At this point the procedures walked you through the setup of the import utility for importing users and group updating the configuration settings. If you select save and error is displayed it will be due to problems with the definitions of groups in your LDAP directory.

16. ___ Select **Exit** to quit the import utility, your entries are already saved.

17. ___ Based on the import time defined, you should see the additional user1 now defined as a user in Content Manager.

8.1

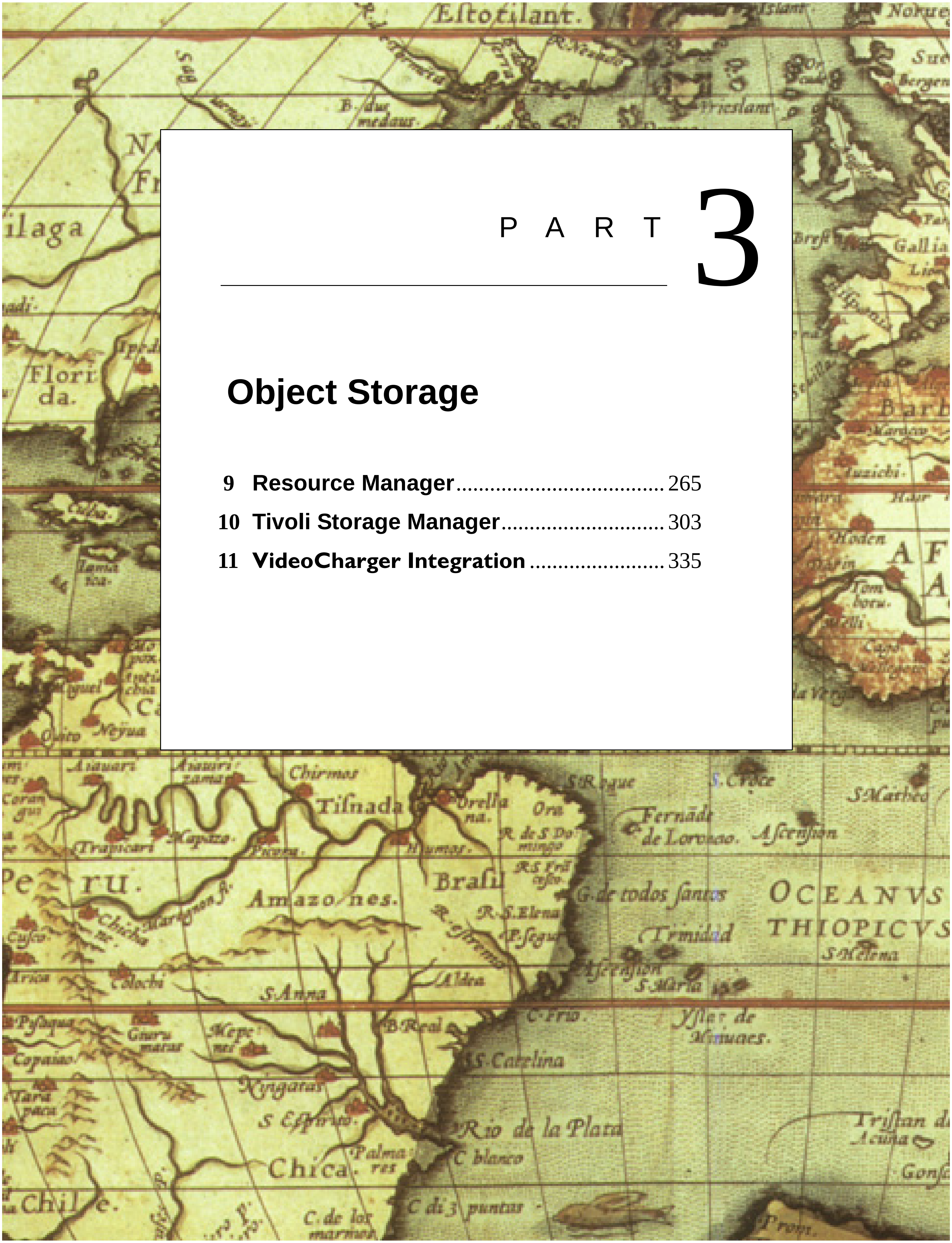
Note: If you use the system administration client to modify a user or group imported from LDAP using the import utility, the modifications will not be replicated to the LDAP directory. For example, if you move a user from one group to another in Content Manager the import utility will re-create the user in the original group that matches the user's association in the LDAP directory. In essence make modifications in the LDAP directory so they are replicated to the Content Manager database.

Summary

The IBM$^{(R)}$ Directory Server Version 4.1 was used to demonstrate how Content Manager connects to an LDAP directory for importing users. LDAP enablement could have also been setup when installing Content Manager if an LDAP directory existed at install time. Refer to the *Planning and Installing Your Content Management System (GC27-1332)* guide for information on installing Content Manager with LDAP.

With the Content Manager LDAP feature enabled, Content Manager will use the LDAP directory to authenticate the user ID and password for accessing the system. The rights the user has within Content Manager are still defined in the Content Manager user profile that is linked to the LDAP person unit or user.

With LDAP enabled for Content Manager, care needs to be given as to how user information is updated, especially when adding and deleting users. If the Content Manager LDAP import utility is being used to create the user profile records in Content Manager, then any addition or deletion of users should be done in the LDAP directory. Doing this makes sure the actions taken to delete and add users in LDAP are replicated to Content Manager. Removing and adding users directly in Content Manager does mean they will be replicated back to the LDAP directory. In fact, users deleted in Content Manager and not removed from the LDAP directory will be re-created in Content Manager the next time the Content Manager LDAP import utility runs.



PART 3

Object Storage

CHAPTER 9

Resource Manager

- Architecture
- Managing the Resource Manager
- Object Storage Configuration
- Resource Manager Services

*I*n this chapter, you will learn about the resource manager server in detail. The server architecture and differences from previous versions of Content Manager will be presented. You will also learn how to manage and configure different storage requirements. The resource manager services, and their role will be discussed in detail. The goal of this chapter is to not only introduce you to the role of the resource manager server, but to also provide the level of knowledge required to install and maintain one. The concepts learned here will be applied in the following chapters where the integration with Tivoli Storage Manager and VideoCharger are discussed.

Architecture

The resource manager server is used to manage the storage and delivery of the physical objects (i.e. documents, images, videos, audio) in your Content Manager system, and is a replacement to what was once called an object server in previous versions of Content Manager. The resource manager server is implemented as a J2EE application and is supported to run under WebSphere Application Server V4.0.3.

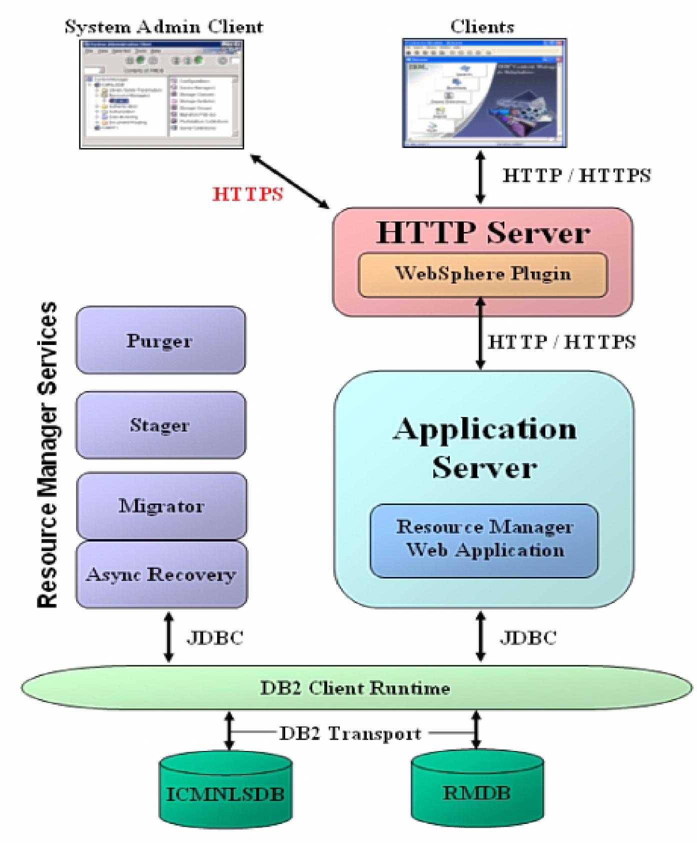


Figure 9-1 *Resource Manager Architecture*

Figure 9-1 depicts the resource manager architecture and how it interacts with other components in your Content Manager system. Notice that the resource manager is a web application which runs inside an application server. WebSphere Application Server Advanced Single Server Edition (AEs) only allows you to define a single application server. WebSphere

Application Server Advanced Edition (AE) allows you to define more than one application server. When started, the application server will appear as a java.exe process in your operating system list of running processes. An application server can host more than one web application. Therefore, in the case of WebSphere Application Server AEs, the single application server can host both the resource manager and eClient web applications.

As Figure 9-1 shows, the resource manager communicates directly with both the library server and resource manager databases. This communication is facilitated by a JDBC connection. The JDBC driver is installed by the DB2 Runtime client. The physical location of these databases does not matter. However, whether they exist locally or remotely, the resource manager web application must be able to use the DB2 Runtime client JDBC driver to access both databases.

The resource manager services (discussed in detail later in this chapter) are run as separate processes along-side the resource manager web application. The migrator and asynchronous recovery tool also require JDBC access to the databases, as they need to make database changes.

As the resource manager server is implemented as a web application, clients communicate with the server using either the HTTP or HTTPS protocol. The Content Manager System Administration client will only communicate with the resource manager using HTTPS, and therefore requires that a secured sockets layer (SSL) be configured between the client and the resource manager web application. Other clients can communicate with the resource manager with either HTTP or HTTPS (the Windows Client using HTTP).

Note: The Content Manager System Administration client will only communicate with the resource manager using HTTPS, and therefore requires that a secured sockets layer (SSL) be configured.

It is important to realize that these transport links exist even if all components are installed on a single machine. This means that the clients will still use either the HTTP or HTTPS protocol to communicate with the resource manager, and the resource manager will still require a JDBC connection to the local databases. Keeping this point in mind is key to troubleshooting and understanding the overall architecture of the resource manager server.

This architecture allows for many improvements over the previous object server architecture found in earlier versions of Content Manager. Some of these improvements include:

- Use of standard protocols for communication (HTTP, HTTPS, XML, FTP, HTML)
- No destager
- Threaded migrator
- Much heavier reliance and use of the database manager features

Being a web application, communication with the resource manager is made via HTTP POST and GET requests to the web application servlets. The request and response information are in XML format, while the actual document can be stored or retrieved by either HTTP or FTP (although HTTP is the default method). The access protocol used to communicate with the resource manager is extensible, which allows for implementation of future protocols. By using standard protocols such as HTTP for communication, clients will experience fewer problems with firewalls.

The resource manager does not contain a destager process. Newly imported documents are immediately placed in their first storage location. If the first storage location is not available, then the document import will fail. By removing the temporary destaging area for new documents, the overhead of running a destager process is no longer needed.

The migrator process (discussed in detail later in this chapter) leverages the threading model of JAVA and creates a separate thread for each volume in the system when work needs to be done. In previous versions of Content Manager, the migration of documents was handled serially (no matter how many volumes were involved). By creating a thread for each volume, the migrator process can work with different volumes in parallel, and thereby decrease the amount of time needed to migrate a set of documents.

When created, the resource manager database will automatically exploit database manager features to allow for both speed and scalability. For example, a separate tablespace will be automatically created for the larger resource manager tables, and indexes will be created on table columns that are used extensively in queries.

The new architecture of the resource manager server allows you to more easily meet the needs of today’s web based clients, while still facilitating easy access for the desktop client applications. By utilizing the scalability of WebSphere Application Server for cloning and clustering, a single resource manager can grow to meet the needs of your company. Furthermore, the performance monitoring tools of WebSphere and DB2 allows you to ensure that the resource manager is operating efficiently.

Managing the Resource Manager

In order to maintain a resource manager server, you should be aware of certain concepts and tasks. In this section, you will continue the architectural discussion by applying the previously introduced concepts to real world tasks. The steps needed to manually deploy the resource manager web application and start/stop the resource manager server will be presented. You will also take a closer look at the access protocols, and how the resource manager handles security.

Manual Deployment

When installing a resource manager server, the installation program will automatically deploy the resource manager web application into WebSphere Application Server (AE or AEs). However, you do have the option of deploying the web application yourself. This may be needed if you decide to perform WebSphere configuration or maintenance. You may also need to manually deploy the resource manager if the installation program failed to do so.

Being a web application, the resource manager is packaged as a web application resource file (icmrm.war) and can easily be manually deployed in WebSphere using the deployment wizards.

Note: You may also notice Enterprise Application Resource (EAR) files. These files are made up of one or more web application resource (WAR) files.

The exact procedure for deployment depends on the edition of WebSphere Application Server being used (although the concept is the same).

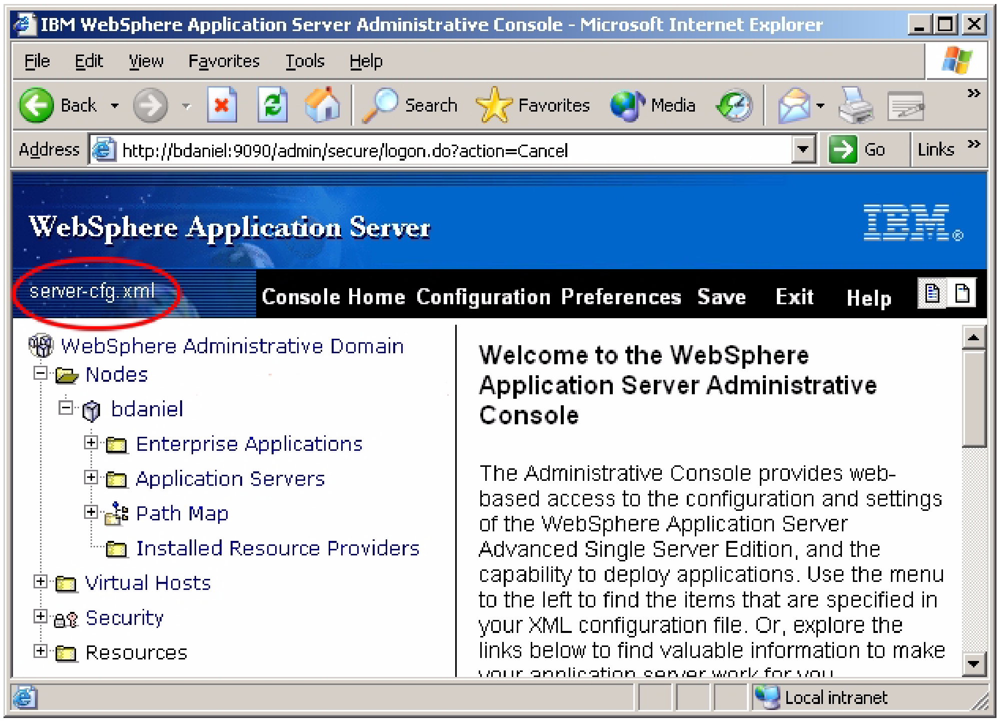
WebSphere Application Server AEs

The following steps describe how you can manually deploy a resource manager server in WAS AEs:

1. ___ If not already started, start WebSphere Application Server AEs by selecting **Start | Programs | IBM WebSphere | Application Server V4.0 AEs | Start Application Server**.

2. ___ Go to the WAS Administrative Console by selecting on **Start | Programs | IBM WebSphere | Application Server V4.0 AEs | Administrator's Console**.

3. ___ Logon using any name as it is only used for logging purposes.



IBM WebSphere Application Server Administrative Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://bdaniel:9090/admin/secure/logon.do?action=Cancel
Go Links
WebSphere Application Server
IBM
server-cfg.xml
Console Home Configuration Preferences Save Exit Help
WebSphere Administrative Domain
Nodes
bdaniel
Enterprise Applications
Application Servers
Path Map
Installed Resource Providers
Virtual Hosts
Security
Resources
Local intranet

Welcome to the WebSphere Application Server Administrative Console

The Administrative Console provides web-based access to the configuration and settings of the WebSphere Application Server Advanced Single Server Edition, and the capability to deploy applications. Use the menu to the left to find the items that are specified in your XML configuration file. Or, explore the links below to find valuable information to make your application server work for you

Figure 9-2 *WebSphere AEs Configuration File*

When configuring Websphere AEs, be sure that you are working with the correct configuration file. The configuration file you are currently working with appears in the upper left hand corner (shown in Figure 9-2). WebSphere AEs stores all its information in an XML file, which is named server-cfg.xml by default. This gives you the capability of creating other configuration files to hold separate WebSphere configurations.

The resource manager will be deployed into the default server-cfg.xml configuration. (So you may continue to work with the default configuration file for now.) The eClient installation program will create its own configuration file named IDM_ICM.xml (located in C:\Program Files\IBM\Cmgmt by default). This new configuration file will contain the eClient and resource manager web applications. The eClient will also create a batch file which will start WebSphere AEs using the new configuration file. This is important to remember, because if you want to work with the eClient configuration file, you must select **Configuration** and open the corresponding xml file.

Note: When working with WAS AEs, you must be very patient! After selecting a link, it takes a few moments to get a response.

4. ___ Expand **Nodes**, and then the icon labelled as your **hostname**.

5. ___ Select **Enterprise Applications**.

6. ___ On the right pane, select **Install**.

7. ___ On the top window (labelled “***Specify the Application or Module located on this machine to upload and install***”), specify the following values, and then select **Next** to continue:

Path: C:\Program Files\IBM\CM81\Config\icmrm.war
Application Name: icmrm
Content Root: icmrm

8.1

Note: The application name and context root you specify should correspond to what you specified during the install. Otherwise, the library server will not be able to communicate with the Resource Manager.

8. ___ Leave the virtual host name as **default_host**. Change the *Precompile JSPs* option to **NO**. (This will save time as you will not have to wait for all the JSPs to be compiled. Instead the JSPs will be compiled as they are needed for client requests.) Select **Next** to continue.

9. ___ Select **Finish** to confirm your settings and to start the deployment. This will take some significant time, so be patient.

When the deployment is complete, you will see the following two messages:
"*Configuration needs to be saved*"
"*Plug-in configuration needs to be regenerated*".

10. ___ Regenerate the plug-in configuration by selecting the message labelled "**Plug-in configuration needs to be regenerated**". (Alternately, you can expand the folder labelled Application Server, select Default Server, and then select the Web Server Plug-In Configuration link.) Select **Generate**.

11. ___ Save the new web application to the configuration file (server-cfg.xml) by selecting the message labelled "Configuration needs to be saved." (Alternately, you can select Save from the console menu bar.) Select **OK** to save the configuration file C:\WebSphere\AppServer\config\server-cfg.xml.

12. ___ Before closing the browser window, select **Exit** to exit the Administrative Console. (It is a good practice to always exit the Administrative Console before closing the browser window.)

At this point, you have manually deployed the resource manager server as a web application named icmrm. Before the resource manager can be started successfully, you may need to restart WebSphere. Refer to the next section for steps on how to start and stop the resource manager.

WebSphere Application Server AE

The following steps describe how you can manually deploy a resource manager server in WAS AE:

1. ___ If not already started, start WebSphere Application Server AE by selecting **Start | Programs | IBM WebSphere | Application Server V4.0 AE | Start Application Server**.

2. ___ Go to the WAS Administrative Console by selecting **Start | Programs | IBM WebSphere | Application Server V4.0 AE | Administrator's Console**.

   Unlike WAS AEs, WAS AE stores all its information in a database and allows you to run multiple application server instances.

3. ___ Create an application server instance for the resource manager web application by selecting **Console | Wizards | Create Application Server** from the menu bar.

4. ___ Type **icmrm** as the application server name and select **Next**.

5. ___ As you do not need to enable any other server, select **Next** to continue.

6. ___ Select Finish to create the application server.

   At this point, you should have an application server named icmrm (see Figure 9-4 on page 275). Next, you need to deploy the resource manager web application into this application server. (You could have used the application server named *default server*, but it is a good practice to isolate the server from the default sample configuration.)

7. ___ Select **Console | Wizards | Install Enterprise Application** from the menu bar.

8. ___ Select **Install stand-alone module (*.war, *.jar)** and specify the follow-

ing values and then select Next:
Path: C:\Program Files\IBM\CM81\Config\icmrm.war
Application name: icmrm
Context root for web module: /icmrm

9. ___ Select **Next** 8 more times to accept the default values.

10. ___ At the *Selecting Application Servers* configuration screen, select the icmrm application server you just created and select **Next**.

11. ___ Select **Finish** to complete the web application installation.

At this point, you have created an application server instance named icmrm. You have also deployed the resource manager as a web application also named icmrm into this application server. Refer to the next section for steps on how to start and stop the resource manager.

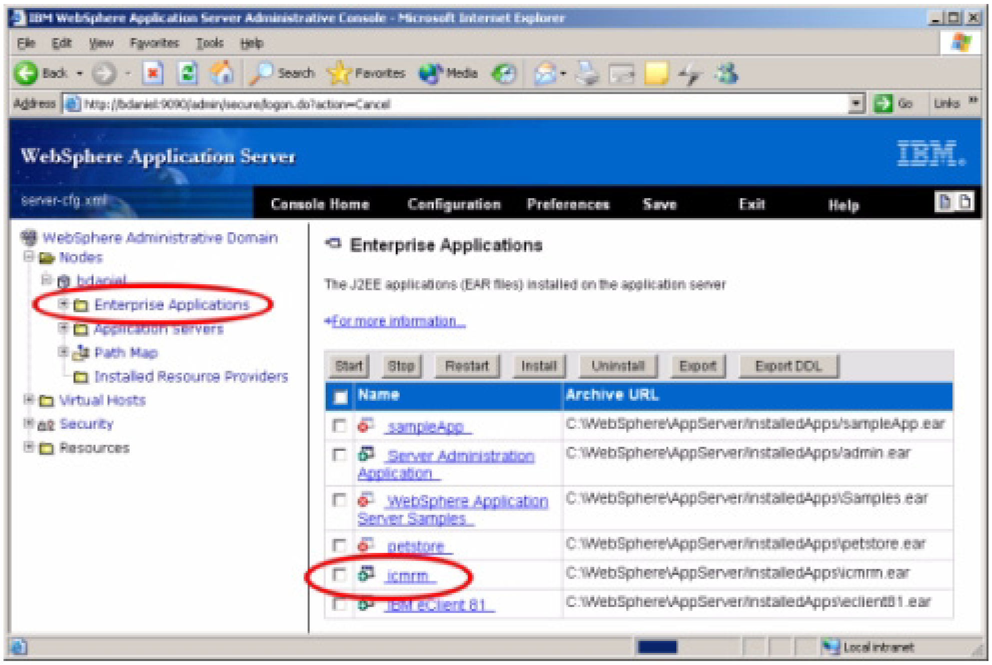
Starting and Stopping

The resource manager server is running when the resource manager web application is running. Recall from Figure 9-1 on page 266 that the web application runs inside an application server. It is important to remember that although the application server may be running, the resource manager web application may not necessarily be. The procedure for starting and stopping the resource manager server depends on the edition of WebSphere Application Server being used.

WebSphere Application Server AEs

12. ___ WebSphere Application Server Advanced Single Server Edition (WAS AEs) allows for only one application server and is managed via a web browser. To start the WAS process and the single application server, select **Start | Programs | IBM WebSphere | Application Server V4.0 AES | Start Application Server**. (This is a shortcut to the startserver.bat file which is located in C:\WebSphere\AppServer\bin by default.)

13. ___ Now that the application server is running, you can use the WAS Administrative Console to start the resource manager web application. To start the Administrative Console, select **Start | Programs | IBM WebSphere | Application Server V4.0 AES | Administrator's Console**. Enter any name to log on as it is only used for logging purposes. In the left pane, expand *Nodes*, machine hostname, and then select **Enterprise Applications**. Your browser window should be similar to that of Figure 9-3 on page 274.


IBM WebSphere Application Server Administrative Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://bdaniel:9090/admin/secure/logon.do?action=Cancel
Go Links
WebSphere Application Server
IBM.
server-cfg.xml
Console Home
Configuration
Preferences
Save
Exit
Help
WebSphere Administrative Domain
Nodes
bdaniel
Enterprise Applications
Application Servers
Path Map
Installed Resource Providers
Virtual Hosts
Security
Resources
Start
Stop
Restart
Install
Uninstall
Export
Export DDL
Local intranet

Enterprise Applications

The J2EE applications (EAR files) installed on the application server

For more information...

☐	Name	Archive URL
☐	sampleApp	C:\WebSphere\AppServer/installedApps/sampleApp.ear
☐	Server Administration Application	C:\WebSphere\AppServer/installedApps/admin.ear
☐	WebSphere Application Server Samples	C:\WebSphere\AppServer/installedApps\Samples.ear
☐	petstore	C:\WebSphere\AppServer/installedApps\petstore.ear
☐	icmrm	C:\WebSphere\AppServer/installedApps\icmrm.ear
☐	IBM eClient 81	C:\WebSphere\AppServer/installedApps\eclient81.ear

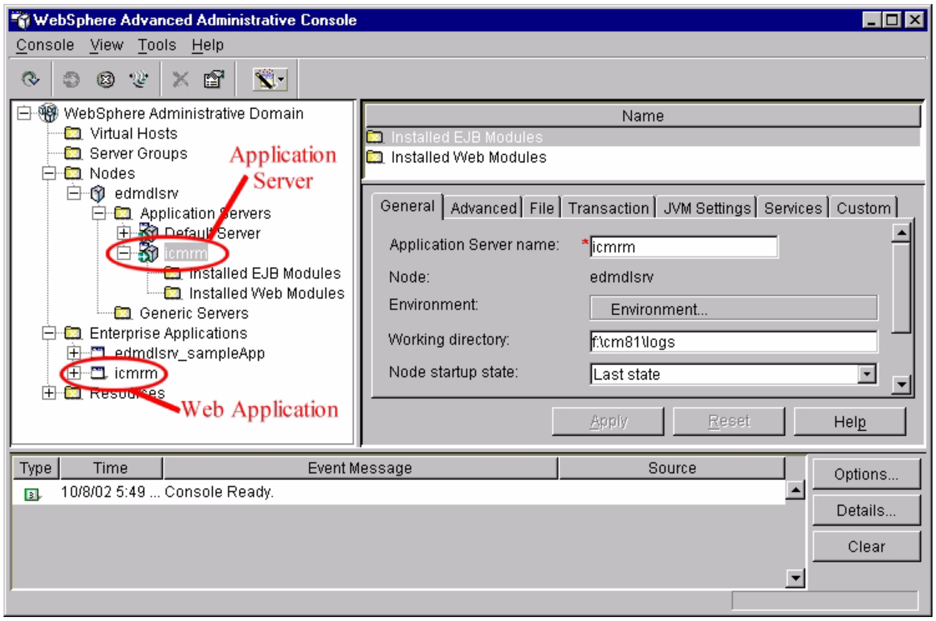
Figure 9-3 *Resource Manager Web Application in WAS AEs Admin Console*

14. ___ By default, the resource manager web application is named icmrm. The web application is running if the arrow next to it is green. Conversely, the web application is stopped if the arrow is red. If needed, check the box next to icmrm and select **start**. After a moment (be very patient with the AEs edition), the resource manager web application should start.

15. ___ To stop the resource manager, you may simply stop the resource manager web application (icmrm). This is done from the window where the web application was initially started (see Figure 9-3). Alternately, you can stop the application server by running **stopServer.bat** (located in C:\WebSphere\AppServer\bin by default). Doing so will stop the application server and all web applications which it hosts.

WebSphere Application Server AE

16. ___ WebSphere Application Server (WAS) Advanced Edition (AE) allows for more than one application server instance. Before any of these application servers can be started, the WAS process must be started by going to *Windows Services Control* Panel and starting the service named **IBM WebSphere**. Once the service has started, launch the Websphere Administrator's Console by selecting **Start | Programs | IBM WebSphere | Administrator’s Console**. A window similar to Figure 9-4 will appear.



Application Server name: *icmrm
Node: edmdlsrv
Working directory: f:\cm81\logs
Node startup state: Last state

10/8/02 5:49 ... Console Ready.

Figure 9-4 *Resource Manager in WAS AE Administrative Console*

17. ___ By default, the application server name which contains the resource manager web application is icmrm. To see a list of defined application servers, from the left pane, expand *Nodes*, *machine hostname*, and then *Application Servers*. An application server is running if the arrow next to it is green. Conversely, the application server is stopped if the arrow is red. If needed, right-click on the icmrm application server and select **start**. After a moment, you should get a message indicating that the server has started successfully.

18. ___ In WAS AE, when an application server starts, it will automatically start the web applications it contains. To see a list of defined web applications, from the left pane, expand *Nodes*, and then *Enterprise Applications*. Unlike the application server, web applications do not have an icon to indicate if they are running or stopped. However, you can check the state of a web application by right-clicking on it and choosing **Status**.

19. ___ To stop the resource manager, you may simply stop the resource manager web application (icmrm). This is done by right-clicking on the icmrm web application and selecting **stop**. Alternately, you can stop the application server by right-clicking on icmrm and selecting stop. Doing so will stop the application server, and all web applications which it hosts.

Secured Sockets Layer (SSL)

Resource manager servers are configured from the System Administration Client (see Figure 9-5). Because the configuration data must be protected, a secure form of communication must be established between the resource manager and the configuration client. This secure form of communication is facilitated by the secured sockets layer (SSL).

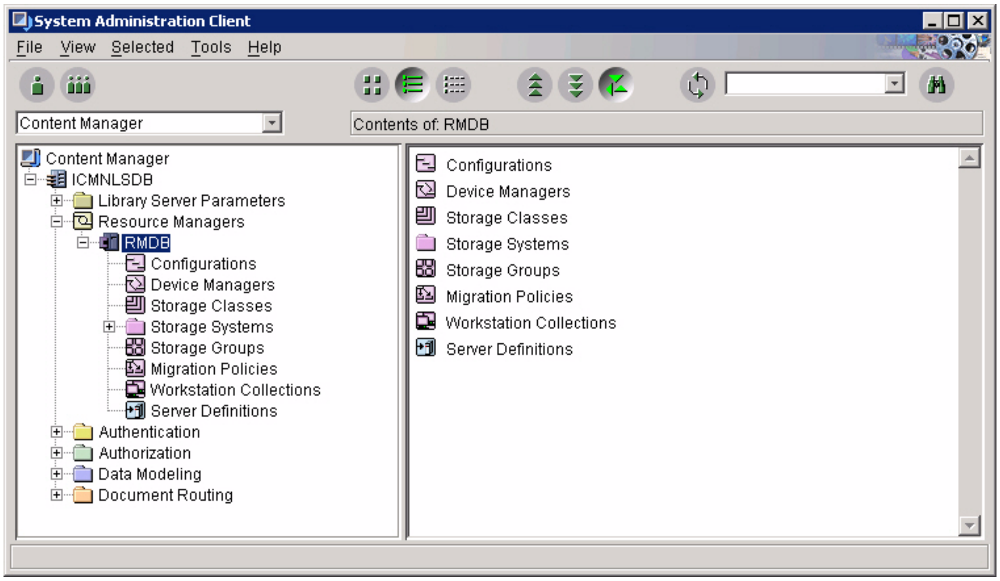


Figure 9-5 *Using Administration Client to Configure Resource Manager*

Note: In order for the System Administration client to be able to communicate with a resource manager, SSL must be properly configured. SSL is only needed for configuration, and is NOT required by regular clients to store / retrieve documents.

When you select a resource manager in the System Administration client, a SSL connection is attempted. If the SSL connection cannot be made, then an error message will be shown (even though the resource manager may be running and configured). The steps for configuring SSL with the IBM HTTP Server can be found in Chapter 18 of the publication entitled *Planning and Installing Your Content Management System* (GC27-1332). Chapter 3 of this publication also contains an exercise to walk you through the SSL configuration.

Although any HTTP Server which is supported by WebSphere Application Server can be used, the Content Manager publication only includes the steps for configuring IBM HTTP Server with SSL. Therefore, if you decide to use another HTTP Server, you must rely on its documentation to describe how SSL should be configured.

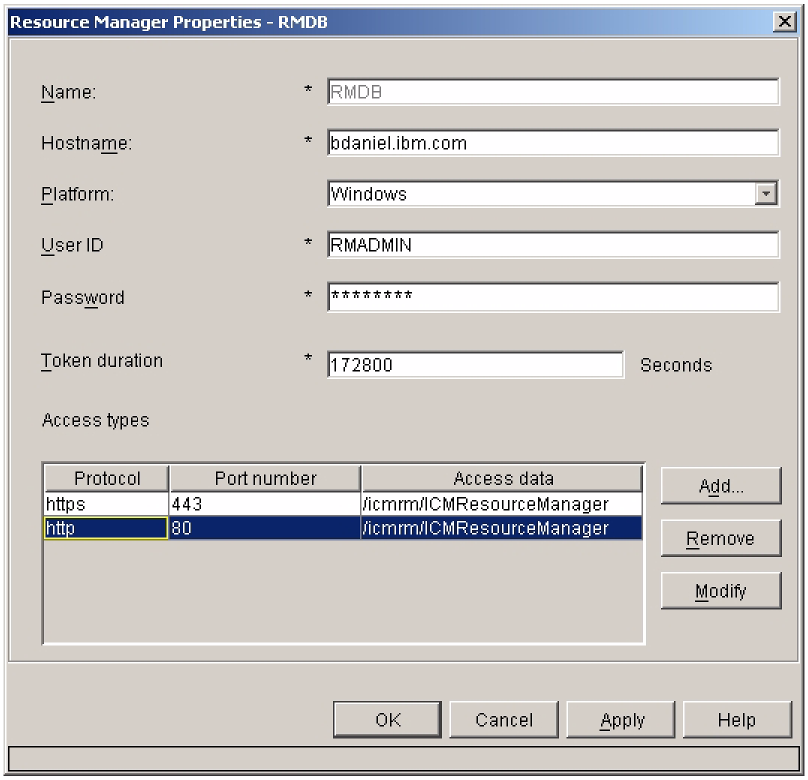
Updating Resource Manager Properties

The information needed to access the resource manager server can be updated from the Content Manager System Administration Client. Such information includes the hostname, database user ID/password, token duration, and the access types. To update these values, right-click on the **resource manager server**, and choose **properties**. The resource manager properties window (see Figure 9-6) will appear.

Most of these values should look familiar to you, as they were specified during the Resource Manager installation. The hostname specifies the location of the resource manager server and should be accessible by all client machines. Therefore, you should always use the fully qualified hostname (i.e. cmv8pc.ibm.com) and not just the short name (i.e. cmv8pc). You may also choose to specify the IP address instead of the hostname.

Note: You should be able to go to a command window, and ping the hostname value specified. For example, "ping cmv8pc.ibm.com" should be successful from ALL client machines.

The userid and password specified is what the resource manager web application will use to connect to the resource manager database (RMDB). This is the system userid that was created before the Content Manager installation and is the one which must have database administrative authority. The userid and password specified here is saved in the icmrm.properties file (the password is encrypted). If you ever need to update the userid and/or password used by the resource manager to connect to the database, you can either do it from this window or directly edit the icmrm.properties file.



Resource Manager Properties - RMDB

Name:	*	RMDB	
Hostname:	*	bdaniel.ibm.com	
Platform:		Windows	
User ID	*	RMADMIN	
Password	*	********	
Token duration	*	172800	Seconds

Access types

Protocol	Port number	Access data
https	443	/icmrm/ICMResourceManager
http	80	/icmrm/ICMResourceManager

Figure 9-6 *Resource Manager Properties Window*

8.1

Note: The icmrm.properties file is read by the resource manager when it needs the database userid and password. If the SysAdmin client is not available, you can update the password in this file and it will be automatically re-encrypted by the resource manager.

From this properties window, you can also specify how long tokens are to remain valid. In the next section, you will learn what a token is and how it is used by the resource manager.

The access types specify how clients can access the resource manager. Table 9-1 on page 279 shows the default access types.

Table 9-1 *Default Resource Manager Access Types*

Protocol	Port	Access Data
https	443	/icmrm/ICMResourceManager
http	80	/icmrm/ICMResourceManager

The HTTPS protocol allows for secured communication and is used by the System Administration client for resource manager configuration. The HTTP protocol is used by regular clients (i.e. Windows Client) to access the resource manager. Remember, the resource manager server is a web application and is therefore accessed as such.

Notice that the port and URL for each protocol is specified. For example, in the configuration depicted in Figure 9-6, to access the resource manager server using the HTTPS protocol, *https://cmv8pc.ibm.com:443/icmrm/ICMResourceManager* would be used. Likewise, to access the resource manager using the HTTP protocol, *http://cmv8pc.ibm.com:80/icmrm/ICMResourceManager* would be used.

8.1

Note: To configure client request to go straight to WAS (thereby bypassing the HTTP Server completely), change the HTTP protocol port from 80 to the port used by the icmrm web application in WAS.

If you wanted client requests to go straight to the resource manager web application (thereby bypassing the HTTP Server completely), you can alter the port for the HTTP protocol. For example, the default port used by the resource manager server under WebSphere AEs is 9080. If you change the HTTP protocol port from 80 to 9080, then all client requests (to store and/or retrieve documents), would be sent directly to WebSphere via *http://cmv8pc.ibm.com:9080/icmrm/ICMResourceManager.*

If you are not quite clear on how ports are used between the HTTP Server and WebSphere Application server, please refer to the resource manager troubleshooting section for a more in depth discussion.

Tokens and Access Control

The resource manager server uses what is referred to as a *token* to validate the authenticity of client requests. A unique token is dynamically generated by the library server for each client request and will remain valid for a set length of time. View tokens as temporary keys used to access particular documents stored on a resource manager. In order to better understand how tokens are used, examine what happens when a client requests a document.

When a client wants to retrieve a document, the request is first sent to the library server. The library server contains the access control information (i.e. privilege sets, access lists, etc.) and also knows which resource manager the requested document is stored on. (Remember, a Content Management system could have more than one resource manager server.) If the library server determines that the client is authorized to retrieve the document (by checking the access control lists), then the library server will generate and encrypt a token for this particular request. This token, and the resource manager information (i.e. hostname, port, access data) will be passed back to the client. The client will then send the request to the designated resource manager server, being sure to pass the token as well. The resource manager server will decrypt the token and validate it. If the token passes verification, the resource manager server will send the requested document to the client.

The library server generates a unique token for each request. This means that if the same client makes two requests for the same document, then two distinct tokens will be generated.

If you are still unsure how a token is passed the resource manager, take a look at the following URL:

```
http://cmv8pc.ibm.com/icmrm/ICMResourceMan-
ager?order=retrieve&item-id=A1001001A02I14B35246C66013&ver-
sion=1&objname=L1.A1001001A02I14B3546C66013.V1&collection=C
BR.CLLCT001&lib-
name=ICMNLSDB&token=A4E6.DPeOEk6_zQGPKXZmRvw;&content-
length=0
```

This is an example of how the Content Manager eClient Version 8 will request a document from a resource manager. The request is made via HTTP to the ICMResourceManager servlet and includes numerous parameters, one of which is the token *A4E6.DPeOEk6_zQGPKXZmRvw*. The string of characters will be decrypted and verified by the resource manager before it honors the retrieve document order.

Once the client has a valid token, it can be used over and over to perform the same request. This fits in nicely for web applications that dynamically generates links for documents. A client may retrieve the document multiple times without having to obtain a new token from the library server each time. This greatly reduces the amount of traffic that must go on between servers and clients. However, this token cannot be used by the client indefinitely.

The length of time which a token will remain valid, the token duration, can be adjusted from the resource manager properties window (see Figure 9-6 on page 278). By default, a token will be valid for 48 hours before it expires. Once a token expires, it can no longer be reused and the client must request a new token from the library server. You should always allow a token to expire. The reason for this is that once a client has obtained a token to retrieve a document, the token can be used to access the document even after the access control in the library server has been altered to restrict access. Remember, the token is a key to a document in the resource manager. Once the key is valid, the client can continue to use it to retrieve the document.

In order to be able to decrypt tokens, the resource manager encryption keys must correlate with the library server encryption keys. You should periodically regenerate new encryption keys (especially if your clients include Internet users). Encryption keys can be regenerated from the library server configuration and should only be performed when ALL resource manager servers are up and operating properly.

8.1

Note: Encryption keys should only be regenerated when ALL the resource manager servers are up and operating properly.

When you regenerate the encryption keys, the library server will first generate a new set of keys. It will then send this information to the resource manager servers. If a resource manager server is not running (or not functioning properly), then it will not obtain the new set of keys. As a result, it will never be able to decrypt any new tokens, and will always throw an error message similar to *The security token supplied with order store was invalid*. Also, once a resource manager obtains a new encryption key, it will not be able to decrypt tokens which may have been previously given to clients. As a result, even if the old tokens have not yet expired, clients will need to obtain a new token (which uses the new encryption key) from the library server.

Staging Area

The *staging area* is specified during installation and is used by a resource manager server as a cache for documents stored within a Tivoli Storage Manager (TSM) server. This provides fast access to documents which would normally be stored on slower media (such as optical platters).

When a client requests a document that is stored within TSM, the resource manager would retrieve the document from TSM into the staging area and send it to the client. This initial request may take a noticeable amount of time, especially if the document is stored on an unmounted volume in TSM. However, because this document now exists in the staging directory, any future requests for this particular document will be handled much faster.

The staging area is created when you install Content Manager and is, by default, located in C:\Staging. From the System Administration client, you can change the staging area location, the maximum size, and the purging thresholds (see Figure 9-11 on page 295).

8.1

> **Note:** The staging area is no longer used as a temporary storage location for imported documents. Instead, new documents are placed directly into their first storage location.

You will learn how to configure the staging area in the section entitled *Resource Manager Services*.

Object Storage Configuration

In this section you will be introduced to the entities that make up an object storage configuration. The resource manager configuration is very versatile, but can be somewhat confusing for first time users. However, understanding the building blocks of the object storage configuration is quite easy, and will quickly allow you to define various policies for how documents are to be stored on a resource manager.

The diagram in Figure 9-7 depicts an object storage configuration example. This example will be referred to in the following sections, which describe the different blocks and the functions they serve. As you read through the remainder of this section, keep referring to this diagram as you learn about the different object storage entities.

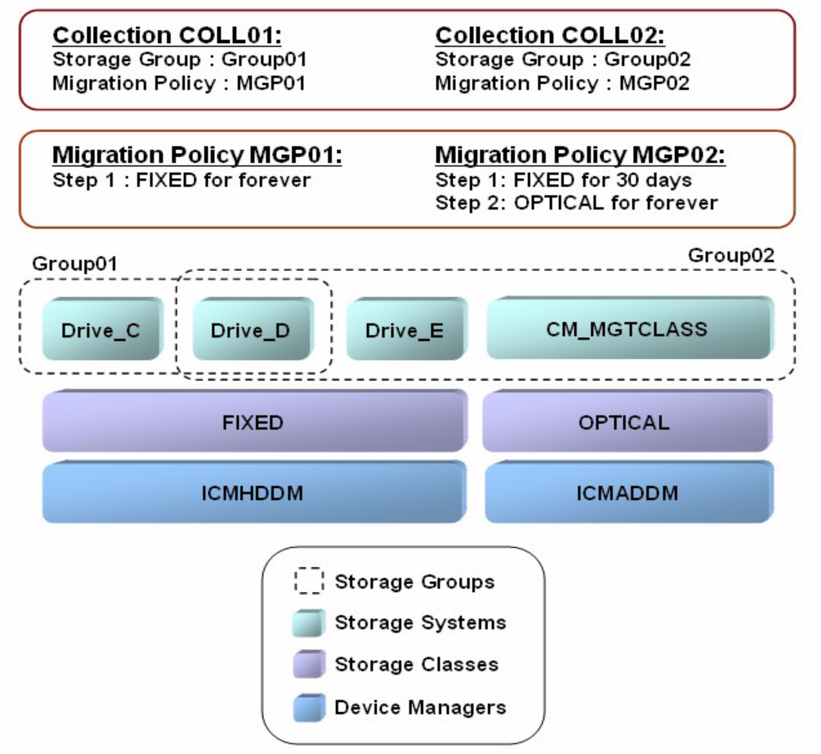


Figure 9-7 *Example Object Storage Configuration*

In the next chapter, you will apply this knowledge to create a object storage configuration which migrates documents to a Tivoli Storage Manager server.

Device Managers

A *device manager* is used by the resource manager to communicate with the actual physical storage location of documents and is comparable to the SCSI and IDE device drivers of the operating system. Device managers are implemented as java class files and may also make native calls to shared libraries (DLLs). As such, you have the ability to create other device managers to support any unique storage devices. However, this is rarely needed, as Content Manager already includes device managers for all the popular storage mediums.

Table 9-2 shows the device managers that are included with Content Manager. Notice that some device managers are only available on certain platforms.

Table 9-2 *Device Managers Shipped With Content Manager*

Device Manager	Description
ICMHDDM	Windows hard disk
GPFS	AIX (version 5) GPFS volumes
JFS	AIX and Solaris JFS volumes
ICMMADM	Media Archiver
OAM	OS/390
ICMADDM	Tivoli Storage Manager (TSM)
ICMVCDM	VideoCharger
ICMFILEPATH	Used to catalog files (external reference)
ICMREMOTE	Remote Server

Not all device managers correspond directly to a physical storage medium. For example, the ICMHDDM device manager is used by the resource manager to access documents stored on Windows hard disks. On the other hand, the ICMADDM device manager is used by the resource manager to access documents that are managed by a Tivoli Storage Manager Server, described in the next chapter.

Device managers can either be enabled or disabled via the Content Manager System Administration Client. Naturally, if a device manager is disabled, then the resource manager has no way of either storing or retrieving documents from the respective storage device. A device manager may be disabled simply because it is not needed, or to perform maintenance on the storage device.

In the example depicted in Figure 9-7, two device managers, ICMHDDM and ICMADDM are enabled. The ICMHDDM device manager is used to access the hard disks while the ICMADDM device manager is used to communicate with the Tivoli Storage Manager server.

Note: By default, only the ICMHDDM and ICMFILEPATH device managers are enabled.

Storage Classes

A *storage class* identifies the destination (local or remote) and type of media that an object is stored on. Storage classes can be associated with either a local or remote destination. A local destination is specified by associating the storage class with a device manager. A remote destination is specified by associating the storage class with another resource manager. Because the storage class name is later used to define document migration policies, you should name your storage classes in accordance with the storage medium. For example, it makes sense to name a storage class FIXED when it is associated with the hard disk device manager (ICMHDDM). However, it makes little sense to name a storage class CDRIVE when it is associated with the VideoCharger device manager (ICMVCDM). Table 9-3 shows typical storage class names and what they describe.

Table 9-3 *Examples of well defined storage class names*

Name	Describes
FIXED	Hard disk managed by ICMHDDM
OPTICAL	Optical platters managed by ICMADDM
TSM	Various storage media managed by ICMADDM
RM-DFW	Media managed by a remote resource manager named DFW

Note: A storage class can be associated to only one device manager.

In the example depicted in Figure 9-7 on page 283, two storage classes, FIXED and OPTICAL are defined. The FIXED storage class is associated with the ICMHDDM device manager. Likewise, the OPTICAL storage class is associated with the ICMADDM device manager. Because both storage classes are associated with a device manager, we know the storage location is local and not on a remote resource manager. Also, as their name clearly suggests, the FIXED storage class is used to represent the hard disk storage medium, while the OPTICAL storage class is used to represent optical platter storage.

Storage Systems

A *storage system* specifies the location, or volume, of where an object is stored, and is directly associated with a storage class. Therefore, in order to define a new storage system volume, you must first define the associated storage class. The following are four different types of storage systems:

- File System Volume
- VideoCharger Volume
- Media Archive Volume
- Tivoli Storage Manager Volume

A file system volume represents a physical or logical partition of a hard disk. For example, on Windows, a file system volume would be represented by a drive label (i.e. C_Drive). On AIX, a file system volume would be represented by a filesystem mount point (i.e. /home/rmadmin/lbosdata).

.

Note: The file system volume name must be exactly the same as the physical volume label (or mount point).

A VideoCharger volume and a Media Archive volume are used when integrating a VideoCharger Server with the resource manager. The VideoCharger volume represents a VideoCharger Server asset group. Likewise, the Media Archive volume represents the Media Archive Server volume. A detailed discussion of VideoCharger, and why you would want to integrate it with Content Manager, can be found later in this guide.

Lastly, the Tivoli Storage Manager volume is used when integrating a Tivoli Storage Manager server with the resource manager. The Tivoli Storage Manager volume name corresponds directly to the Tivoli Storage Manager Server management class name. A detailed discussion of Tivoli Storage Manager, and why you would want to integrate it with Content Manager, can be found in Chapter 10 of this guide.

Note: You must associate a storage system to a storage group.

When defining a storage system, you must also specify its assignment type. Storage systems can have one of the following three assignments:

- unassigned
- overflow
- assigned

Unassigned

Unassigned identifies a space on a system, but does not assign it to a storage group for use. This means that the volume has been defined, but is not yet usable by the resource manager to store objects. You may choose to leave a volume in the unassigned state if you do not yet want to use the defined space for storage. When you do decide this space is needed, you can easily make it available to the resource manager by assigning it to a storage group.

Overflow

Overflow indicates that this particular storage system volume is available to any storage group which needs more space to store new documents. When a storage system volume becomes automatically assigned to a storage group, the change is permanent.

Assigned

Assigned indicates that the storage system volume space has been allocated for use by the respective storage group. The storage system volume is only available to the resource manager when it is assigned to a storage group, and can be assigned to more that one storage group at any one time.

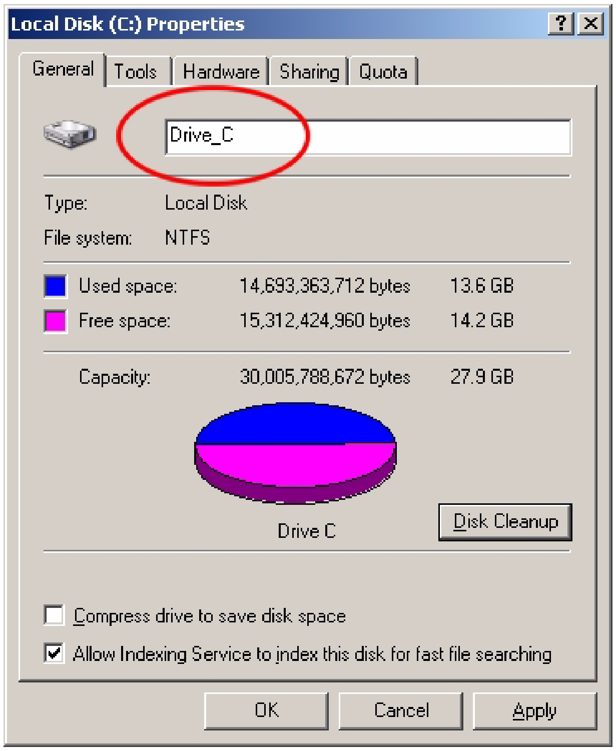
In the example depicted in Figure 9-7 on page 283, two different types of storage systems are defined. There are three file system volumes (Drive_C, Drive_D, Drive_E), and one Tivoli Storage Manager volume (CM_MGTCLASS). Notice that the file system volumes are associated with the FIXED storage class, while the Tivoli Storage Manager volume is associated with the OPTICAL storage class. As the names would suggest, the file system volumes Drive_C, Drive_D, and Drive_E represent C:, D:, and E: respectively. Likewise, the Tivoli Storage Manager volume (CM_MGTCLASS) represents the Tivoli Storage Manager management class named CM_MGTCLASS.

It is important to remember that the file system volume name must be the same as the physical volume label. On AIX, the volume name must be the same as the filesystem mount point.

8.1

Note: If you change the volume label (or replace the hard disk), you must manually update the RMVOLUME table. Exact instructions for doing this can be found in the Content Manager System Administration Guide.

To obtain the volume label on Windows, right click on the drive and choose properties. A window similar to that of Figure 9-8 will appear. If, the file system volume name is not the same as the physical volume label, then the resource manager will not be able to access the volume.



Local Disk (C:) Properties

Drive_C

Type:	Local Disk	
File system:	NTFS	
🟦 Used space:	14,693,363,712 bytes	13.6 GB
🟪 Free space:	15,312,424,960 bytes	14.2 GB
Capacity:	30,005,788,672 bytes	27.9 GB

Drive C

☐ Compress drive to save disk space

☑ Allow Indexing Service to index this disk for fast file searching

Figure 9-8 *File System Volume Label*

Storage Groups

Storage groups are used to specify which storage system volumes can be used by the resource manager to store documents. Storage groups can contain more than one storage system volume. For example, if a storage group named GROUP01 contains two storage system volumes (i.e. Drive_C and Drive_D), then when using GROUP01, the resource manager can store documents on either Drive_C or Drive_D.

Note: The resource manager can only access storage system volumes that are assigned to a storage group.

In the example depicted in Figure 9-7 on page 283, two storage groups, GROUP01 and GROUP02, are defined. Storage group GROUP01 contains two storage systems (Drive_C, Drive_D), while storage group GROUP02 contains three storage systems (Drive_D, Drive_E, and CM_MGTCLASS). Notice that Drive_D is shared between both storage groups. This only defines which volumes are available for a document to be stored on. The decision as to which volume the document will initially be stored on is made by the migration policy.

Migration Policies

Migration policies specifies the rules for migrating documents between storage classes. They consist of a series of steps that a document will take, and specify how long a document will remain at each storage location. Typically, administrators would create a policy which stores new documents on faster hard disks for a certain period of time before moving them off to slower optical platters. The movement of documents between storage classes is handled by the migrator process and will be discussed in the next section.

One of the new requirements of version 8.1, is that the retention period of the last migration step must be set to *forever*. This, in effect, sets the next date that documents must be migrated to 12/31/9999. As a result, the migrator process will never need to look at these documents again. Previously, an administrator could have set this final retention period to anything, such as 30 days. This would have caused the migrator process to inspect documents every 30 days. Because these documents were already at the final storage class, the migrator had no work to do, and thereby wasted precious time looking at these documents in the first place.

Note: Documents will always remain in their last storage class until they are automatically expired by the system, or are manually deleted by end users.

In the example depicted in Figure 9-7 on page 283, two migration policies, MGP01 and MGP02, are defined. Migration policy MGP01 has only a single migration step; to store documents on the FIXED storage class forever. Migration policy MGP02 has two migration steps; to store documents on the FIXED storage class for 30 days, and then move documents to the OPTICAL storage class forever.

Collections

A *collection* consists of a storage group and a migration policy, and is the object storage entity specified for storing new documents into the resource manager. The location for documents in a collection are derived from the storage group and migration policy. Recall that a storage group defines which storage system volumes a particular document can be stored on, and that the migration policy defines the set of rules for moving the document between storage classes. A collection is used to store similar documents in a common location. For example, when you create an item type in Content Manager, you must specify the collection which documents in this item type will use.

Note: You must have a migration policy and a storage group defined to create a collection.

In the example depicted in Figure 9-7 on page 283, two collections, COLL01 and COLL02, are defined. Collection COLL01 consists of the migration policy MGP01 and storage group GROUP01, while collection COLL02 consists for the migration policy MGP02 and storage group GROUP02.

When a document is imported using COLL01, it will be stored on either Drive_C or Drive_D permanently. This information is derived from the migration policy and storage group definitions. The MGP01 migration policy states that documents should be stored on the FIXED storage class forever. The GROUP01 storage group states that documents can be stored on either Drive_C or Drive_D.

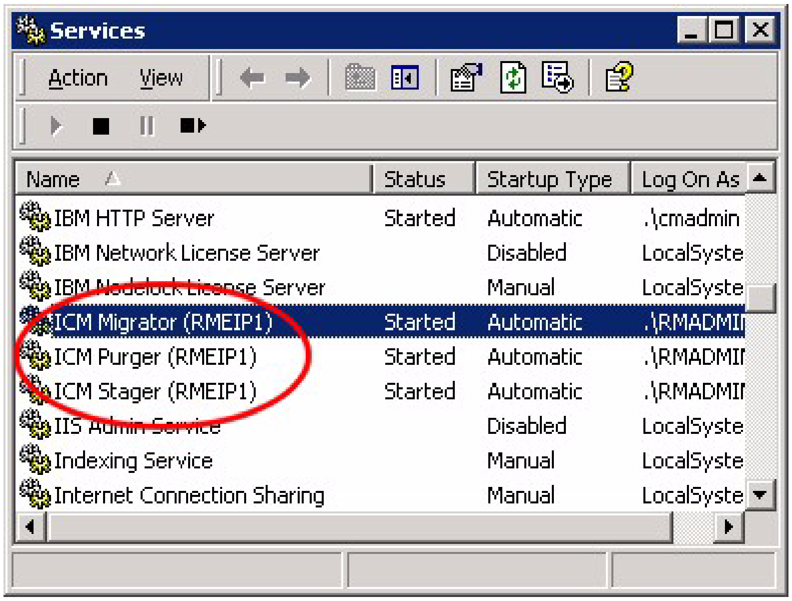
When a document is imported using COLL02, it will be stored on either Drive_D or Drive_E for 30 days, and will then be migrated to the Tivoli Storage Manager volume CM_MGTCLASS permanently. The MGP02 migration policy states that documents should be stored on the FIXED storage class for a period of 30 days before they are migrated to the OPTICAL storage class forever. The GROUP02 storage group states that documents can be stored on either the Drive_D, Drive_E, or CM_MGTCLASS volumes.

The migration policy and storage group used by a collection must have storage systems and storage volumes which coincide with each other. For example, if you create a collection using a migration policy that uses the FIXED storage class, then the storage group used by this same collection must have at least one storage system that is associated with the FIXED storage class.

Resource Manager Services

In this section, we will explore the stager, purger, and migrator services. On Windows, the stager, purger, and migrator services all run as a Windows service and can be started or stopped via the Services Control Panel (see Figure 9-9). On UNIX, these services are run as background processes, and are started from the inittab file.

We will also discuss the asynchronous recovery utilities and how they can be used to ensure the integrity of your library and resource manager databases.



Name	Status	Startup Type	Log On As
IBM HTTP Server	Started	Automatic	.\cmadmin
IBM Network License Server		Disabled	LocalSyste
IBM Nodelock License Server		Manual	LocalSyste
ICM Migrator (RMEIP1)	Started	Automatic	.\RMADMII
ICM Purger (RMEIP1)	Started	Automatic	.\RMADMII
ICM Stager (RMEIP1)	Started	Automatic	.\RMADMII
IIS Admin Service		Disabled	LocalSyste
Indexing Service		Manual	LocalSyste
Internet Connection Sharing		Manual	LocalSyste

Figure 9-9 *Resource Manager Services in Windows Services Control Panel*

Each service requires a unique port number in order to operate properly. Furthermore, the port numbers of the services must be contiguous. In an earlier Chapter, you specified these port numbers during the Resource Manager installation. These specified ports are reserved for use by Content Manager by appending an entry to the file named *services* (located in C:\WinNT\system32\drivers\etc). Take a moment now to open this file in Notepad. Notice that the following lines have been added by the Content Manager installation:

```
RMMigrator_RMDB7500/tcp    #Resource Manager Migrator
```

```
RMPurger_RMDB7501/tcp      #Resource Manager Purger
RMReplicator_RMDB7502/tcp  #Resource Manager Replicator
RMStager_RMDB7503/tcp      #Resource Manager Stager
RMAR_RMDB7504/tcp          #Resource Manager Async Recovery
```

The entries in the services file only reserve these ports. To determine if these are the ports which are really being used, you must inspect the startup command for these services. For example, by viewing the properties of the migrator process, you will see that the startup command looks similar to the following:

```
C:\Program Files\IBM\CM81\BIN\icmnsvrm.exe" RMDB 7500 icmrm
180
```

Notice that the port number to be used is passed as one of its parameters. If you decide to change the port number, it must be changed in both the services file and the startup command of the service.

The resource manager services and the resource manager server are started separately. The resource manager server is not dependent on the services and can even run when all the services are shutdown.

Stager

The job of the *stager* process is to delete staged objects from a VideoCharger server. When using a Media Archive Server with VideoCharger, videos that are archived on the media archive server cannot be directly streamed to clients. When a play request for an archived video is received, the video object must be temporarily staged (or cached) to the Video Charger server. When the VideoCharger stager gets too full, the stager process will delete some, or all, of the staged objects.

Note: Do not confuse the stager process with the staging directory. The stager process has no effect on the staging directory. It is the purger process that affects the staging directory.

Purger

The job of the *purger* process is to maintain the staging area size. Recall that the staging area is used to cache objects from Tivoli Storage Manager and remote resource managers (for LAN Cache). For example, when a client makes a request for a document that is stored in an optical jukebox managed by Tivoli Storage Manager, the document is first copied to the staging directory and then sent to the client. Any future requests for this particular document will be much faster, as the document would then be on the hard disk, and not on a slower optical platter. Also remember that the staging area is not used for new documents. Unlike previous versions of Content Manager, when a document is imported, it is placed in the first storage location specified by the associated collection.

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, Figure 9-10 depicts a 200MB staging area, which has an upper threshold of 190MB and a lower threshold of 10MB. Whenever the staging area reaches 190MB in size, the purger process will begin to randomly delete files from the staging directory, and will continue to do so until the directory reaches 10MB in size.

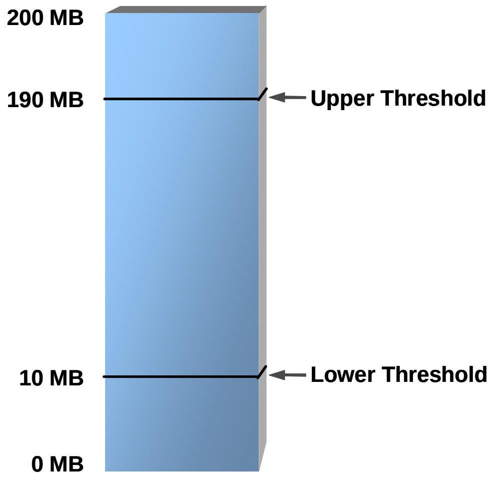
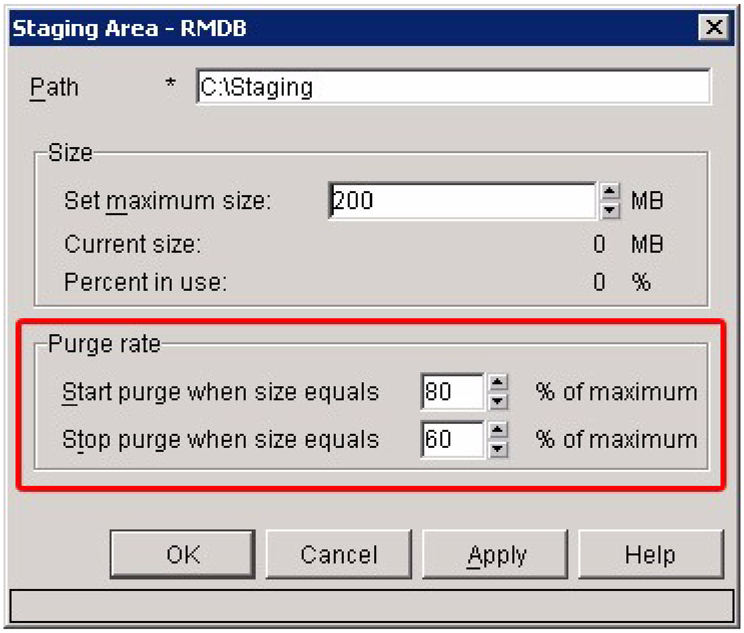


Figure 9-10 *Staging Directory Thresholds*

These thresholds are set when configuring the staging directory in the Content Manager System Administration Client. To view the staging directory properties, right-click on a resource manager server and choose **Staging Area.** The Staging Area Window (see Figure 9-11 on page 295) will appear. Notice that the thresholds are specified as a percentage of the staging area size.



Path * C:\Staging

Size

Set maximum size: 200 MB

Current size: 0 MB

Percent in use: 0 %

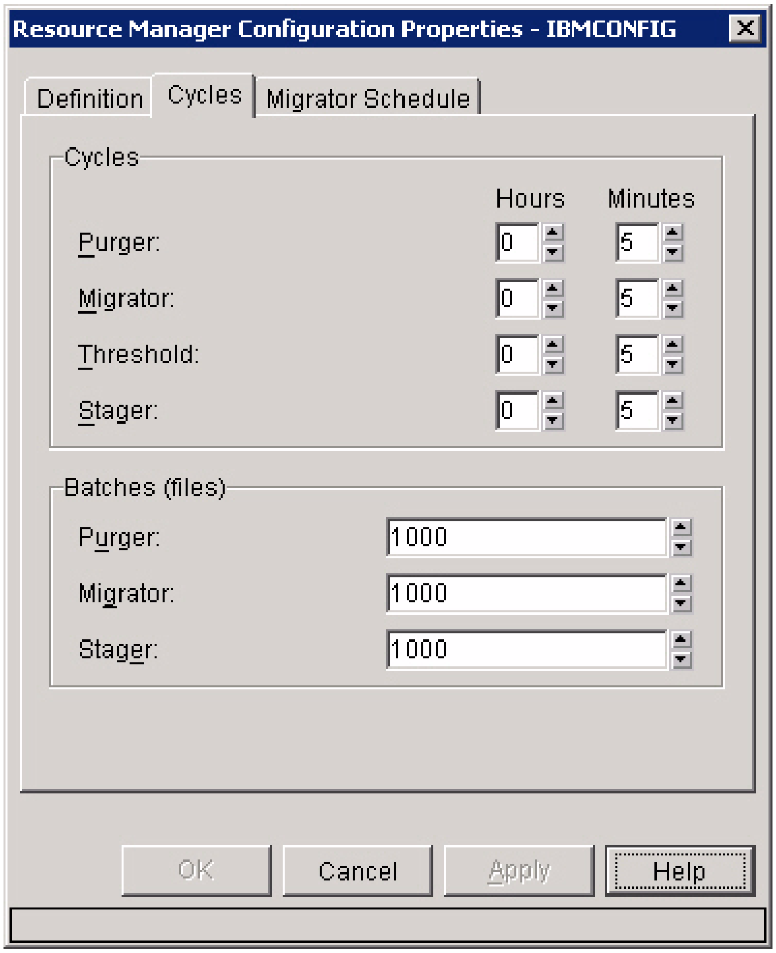
Purge rate

Start purge when size equals 80 % of maximum

Stop purge when size equals 60 % of maximum

Figure 9-11 *Setting the Purger Thresholds*

The staging area size and the threshold criteria are monitored periodically (not constantly). The cycle time is configured via the resource manager configuration. To view the resource manager configuration, from the Content Manager Administration Client, open a resource manager and select the folder labelled **Configurations**. Open the configuration named IBMCONFIG and go to the page labelled **Cycles** (see Figure 9-12 on page 296).



Cycles

	Hours	Minutes
Purger:	0	5
Migrator:	0	5
Threshold:	0	5
Stager:	0	5

Batches (files)

Purger:	1000
Migrator:	1000
Stager:	1000

Figure 9-12 *Cycle time for resource manager services*

The threshold cycle sets the amount of time that must elapse before the staging area size is updated and is set to five minutes by default. This means that the resource manager will obtain the staging area size every five minutes. The purger cycle sets the amount of time that must elapse before the purger process checks to see if it has any work to do and is also set to five minutes by default. This means that every five minutes, the purger process will compare the staging area size against the staging area upper threshold. If the staging area size is greater that the upper threshold, then the purger will begin to work by randomly deleting files until the staging directory size meets the lower threshold.

You may need to adjust the threshold and purger cycle times to meet the needs of your particular environment. For example, in an environment where the staging area is heavily used, you may need to adjust the cycle time so that the purger checks the staging area size more frequently. You may also want to increase the size of your staging directory. However, if your environment does not use the staging area heavily, then you may choose to adjust the cycle time so that the purger performs less checks.

Asynchronous Recovery Utilities

The *asynchronous recovery utilities* consists of two programs which are used for document deletion and transaction reconciliation. These utilities are used to maintain and/or restore the consistency between the library server and resource manager databases. The document deletion utility will determine which documents have been deleted from the library server database (by clients), and will then flag these documents in the resource manager database(s) for deletion. (The migrator will actually perform the removal of database entries for deleted documents.) The transaction reconciliation utility is used to rollback any failed transaction, and ensures that the resource manager database is in synch with the library server database.

These two utilities are automatically executed before the migrator performs any work. However, you do have the option of manually running these utilities yourself. To manually run these utilities, you must perform the following steps:

1. ___ Go to a DB2 command window (located under **Start** | **Programs** | **IBM DB2**).
2. ___ To start the deletion reconciliation utility, run **icmrmdel.bat** (located by default in C:\Program Files\IBM\CM81\bin).
3. ___ To start the transaction reconciliation utility, run **icmrmtx.bat** (located by default in C:\Program Files\IBM\CM81\bin).

It is recommended that you run the asynchronous recovery utilities before performing a backup of your system. This not only ensures your databases are in a consistent state, but also removes any database entries which represent deleted documents.

Tip: After running the asynchronous recovery utilities, run the RUNSTATS function on your databases to ensure that they are operating efficiently.

Migrator

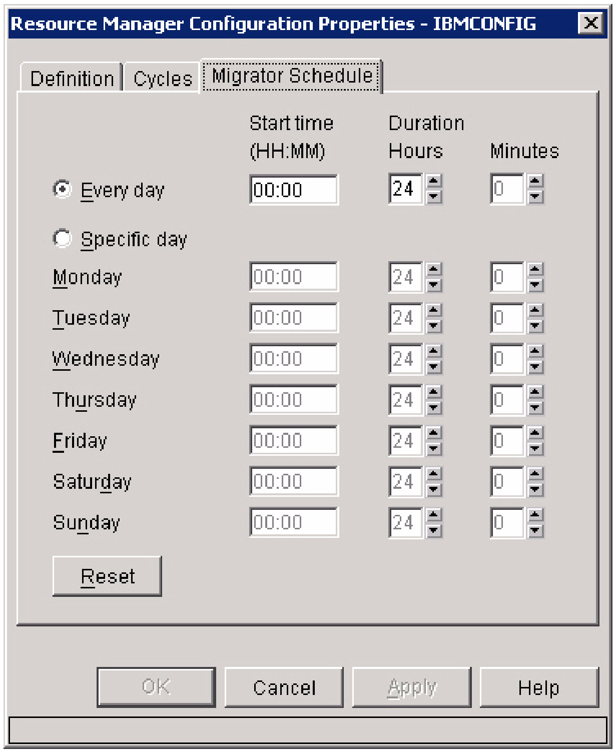
The job of the *migrator* is to move documents between storage classes and to remove deleted documents from the database. Recall from the previous section, that migration policies are part of the object storage configuration, and are used to specify the rules for migrating documents between storage classes. The migrator process is used to execute the rules set forth by the migration policies. Therefore, if you forget to start the migrator process, documents will never be moved.

Note: The migrator process will also remove rows from the resource manager database for documents which have been deleted from the system.

The second job of the migrator process is to remove objects from the resource manager server which have been marked for deletion by the asynchronous recovery utilities. When a client deletes a document, the database entries are immediately removed from the library server but still remain on the resource manager (for performance reasons). The asynchronous recovery tools will mark the objects in the resource manager database which need to be removed. When the migrator starts, it will perform the deletion of these documents from the database. Therefore, even though you may not be planning to migrate documents between storage classes, you should always ensure that the migrator process has been started, so that deleted documents can be removed from the database tables.

Note: Before performing any work, the migrator process will first run the asynchronous recovery tools.

The migrator process does not constantly check for documents that need migrating as doing so would prove to have a big impact on performance. Like the purger process, the migrator is also configured in the resource manager configuration (see Figure 9-9 on page 292). In addition to the cycle time, you must also configure the migrator schedule (see Figure 9-13).



	Start time (HH:MM)	Duration Hours	Minutes
● Every day	00:00	24	0
○ Specific day			
Monday	00:00	24	0
Tuesday	00:00	24	0
Wednesday	00:00	24	0
Thursday	00:00	24	0
Friday	00:00	24	0
Saturday	00:00	24	0
Sunday	00:00	24	0

Figure 9-13 *Configuring the Migrator Schedule*

From this window, you can define when the migrator process will perform work. Because document migration is an intensive process, you may want to adjust the schedule so that the migrator would only be active during times of low system usage (such as at night). By default, the migrator is allowed to migrate documents 24 hours a days, 7 days a week.

Note: If the migrator cannot finish the job (meaning that it cannot migrate all the documents which need migrating) within the time span allotted, then the migrator will just continue where it left off the next time it is allowed to run.

During the scheduled timespan, the migrator process will periodically check for documents that need migrating. The amount of time that must elapse between these checks is configured in this same window on the page labelled *Cycles* (see Figure 9-12 on page 296). Like the purger process, the migrator process has a default cycle value of 5 seconds. This means that during the time when it is allowed to work, the migrator process will check for documents which need to be migrated every five seconds.

At this point, you may be wondering how the migrator process determines if a document needs to be migrated. This is determined by inspecting the OBJ_ACTIONDATE column in the RMOBJECTS table. A row exists in this table for every document that is managed by the resource manager. Take a moment now to look at the RMOBJECTS table (in the resource manager database). Notice that this table contains information for when a document was created, when it was last modified, the current storage location, the next storage location, and when it needs to be migrated.

Note: The original filename and its MIME type can be found in the RMOBJECTS database table.

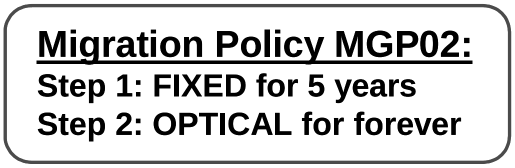
At every cycle, the migrator process will issue a SQL command to select all items from the RMOBJECTS table which have an action date of less than or equal to the current system date. By issuing the following SQL command, you can see which items are waiting to be migrated:

```
db2 select itemid from rmobjects where obj_actiondate <= TODAY
```

Once the migrator uses the actiondate to determine which documents need to be migrated, it will then make other database queries to determine where each document needs to be migrated to. The migration may be between two storage classes on the same resource manager (i.e. FIXED to OPTICAL) or it may be between two resource manager servers (as a storage class can be associated with a collection on another server). Documents are migrated in the order they are returned from the database query.

Note: Any changes to an existing migration policy will not update the action date for existing documents.

Changes to the migration policy are not retroactive. For example, suppose your current system is configured so that the migration policy depicted in Figure 9-14 is used:



Migration Policy MGP02:
Step 1: FIXED for 5 years
Step 2: OPTICAL for forever

Figure 9-14 *Example Migration Policy*

Any new documents will be assigned an actiondate five years from when they were imported. If you then decide to change the retention period for step one from five years down to one year, only newly imported documents will be affected. The existing documents will still retain their original actiondate. If you cannot wait five years for the existing documents to be acted upon by the migrator process, you must manually update their actiondate value.

Summary

This chapter discussed the resource manager server in detail. By first inspecting the architecture, you saw that the resource manager is implemented as a web application, and is supported with WebSphere Application Server. You learned that clients communicate with the resource manager using standard protocols such as XML, HTTP, and HTTPS.

The steps needed to manually deploy and start/stop the resource manager were also discussed. You learned how to configure the resource manager properties, and that a secured sockets layer (SSL) is required for resource manager configuration. A staging area is used as a cache for documents that are stored in Tivoli Storage Manager (which is traditionally used to store documents on slower media such as optical platters).

The resource manager server uses tokens to validate client requests. These tokens are dynamically generated by the library server and are unique for each request. A client may reuse a token to access a particular document until it expires.

The entities required to create a object storage configuration were introduced. Device managers are used by the resource manager to communicate with the actual physical storage location of documents. Storage classes represent the location and storage media for documents and are directly related to a device manager. Storage systems specify the location or volume of where an object is stored and is associated with a storage class. Before a storage system can be used, it must be assigned to a storage group. Storage groups are used to specify which storage system volumes can be used by the resource manager to store documents. Migration policies specify the rules for migrating documents between storage classes. Collections consist of a storage group and a migration policy, and are the object storage entity specified for storing new documents into the resource manager.

The resource manager includes the following services: stager, purger, asynchronous recovery utilities, and migrator. The stager is used to delete staged objects from a VideoCharger server. The purger maintains the size of the staging area. The asynchronous recovery utilities are automatically run by the migrator and are used to maintain and/or restore the consistency between the library server and resource manager databases. The migrator moves documents between storage classes and also removes deleted documents from the database.

CHAPTER 10

Tivoli Storage Manager

- Installing TSM
- Integrating TSM
- Using TSM for Storage
- Troubleshooting

In this chapter, you will be introduced to Tivoli Storage Manager (TSM) and the role it plays in a Content Manager system. You will gain a basic understanding of when to use TSM and how it is integrated with a resource manager. An exercise is included which walks you through the process of configuring this integration. After the integration is performed, you will examine how a document is moved between the resource manager and TSM, and will learn how to troubleshoot integration and migration problems.

Installing TSM

TSM is a client / server program that provides an automated, centrally scheduled, policy managed backup, archival, and space management facility for file servers and workstations. It supports a wide variety of storage devices, some of which include hard disks, manual and automated tape devices, and optical jukeboxes. The powerful storage management system allows documents to migrate between different storage devices, and even allows you to make replica copies of documents (for increased protection from a disaster). TSM includes a set of application programming interfaces (APIs) which allows custom applications to address special storage requirements.

IBM Content Manager leverages the capabilities of TSM by using it to store documents. By itself, a resource manager can only manage documents that are stored on hard disks. By using a TSM server, Content Manager documents can exists on any storage device supported by TSM. Furthermore, TSM features such as copy storage pools and offsite storage can be used.

8.1

Note: If a Content Management system requires documents to be stored on a device other than hard disks (i.e. optical platters), then Tivoli Storage Manager must be installed.

The Tivoli Storage Manager server can be installed on any of its supported platforms, and need not be on the same workstation as the resource manager. Because the resource manager server uses the TSM Client APIs to communicate with a TSM Server, the resource manager and TSM Servers can exists on two different operating systems (i.e. Windows and AIX).

A detailed discussion of the installation and configuration of Tivoli Storage Manager is beyond the scope of this guide. You are encourage to refer to the TSM Publications for a thorough explanation of the TSM concepts and administration tasks.

TSM Server

For the purposes of being able to follow the integration exercise in this chapter, the following steps will walk you through the process of installing and configuring a TSM server. The steps in this chapter assume that you will be installing TSM on the same workstation as the resource manager, and that you will be using the hard disk to store documents managed by TSM (thereby not requiring you to have any special storage requirements).

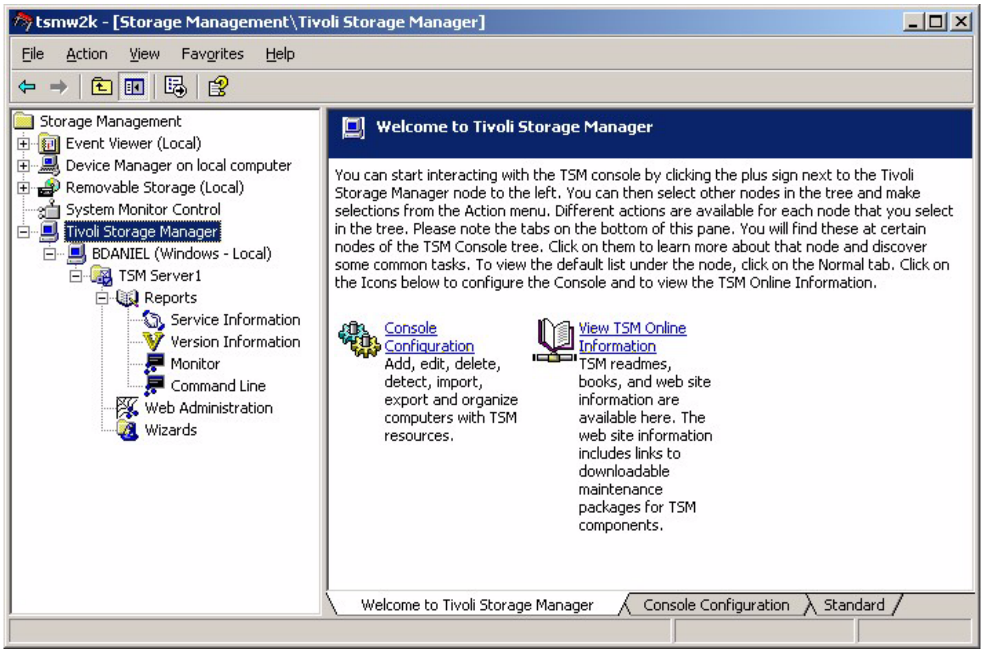
As the purpose of these exercises is to demonstrate the TSM integration with Content Manager, TSM features such as copy storage pools and offsite storage will not be configured.

1. ___ Insert the TSM V5.1 Server CD into your CDROM. The installation program should start automatically.
2. ___ At the Main Menu screen, select **Install Products** and then **TSM Server**.
3. ___ Select **Next** at the TSM Server Welcome Screen.
4. ___ Select **Next** to accept the default destination folder of C:\Program Files\tivoli\tsm.
5. ___ Choose to perform a **typical** install and select **Next** to continue.
6. ___ Select **Install** to begin the file copy process.
7. ___ Select **Finish** to complete the installation. Reboot your computer if prompted.

Now that the Tivoli Storage Manager Server has been installed, it must be configured. The first task is to define a server instance:

8. ___ Open the TSM Management Console by selecting **Start | Programs | Tivoli Storage Manager | Management Console**.
9. ___ Choose **Minimal Configuration** and select **Start**.
10. ___ At the *Welcome to Server Initialization Wizard* window, select **Next** to continue.
11. ___ Select **Next** to accept the default server location of c:\progra~1\tivoli\tsm\server1.
12. ___ Select **Next** to accept the default server volume location.
13. ___ Select **Next** to accept the default server service logon parameters.
14. ___ Select **Next** to accept the default server name (which is based on your workstation hostname).
15. ___ Select **Finish** to complete the server initialization wizard.
16. ___ A message indicating that the server instance was created should appear. You should also see a service named *TSM Server1* in the Windows Services Control Panel.
17. ___ Back on the *Initial Configuration Task List* window, select **Done**. You will

be placed in the TSM Management Console (see Figure 10-1).



You can start interacting with the TSM console by clicking the plus sign next to the Tivoli Storage Manager node to the left. You can then select other nodes in the tree and make selections from the Action menu. Different actions are available for each node that you select in the tree. Please note the tabs on the bottom of this pane. You will find these at certain nodes of the TSM Console tree. Click on them to learn more about that node and discover some common tasks. To view the default list under the node, click on the Normal tab. Click on the Icons below to configure the Console and to view the TSM Online Information.

Console Configuration: Add, edit, delete, detect, import, export and organize computers with TSM resources.

View TSM Online Information: TSM readmes, books, and web site information are available here. The web site information includes links to downloadable maintenance packages for TSM components.

Figure 10-1 *TSM Management Console*

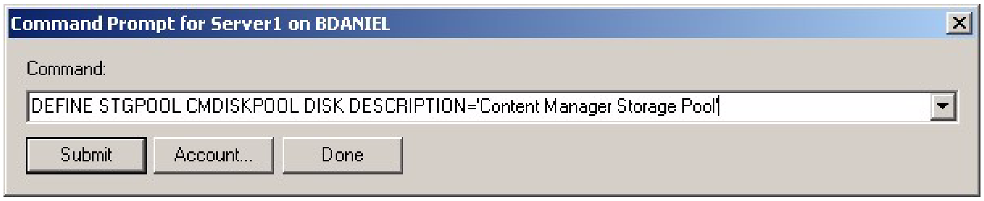
Note: The TSM default administrative userid is **admin**, with a password of **admin**.

Now that a service instance has been defined, you need to create a storage configuration, policy configuration, and a client node for use with Content Manager. The following steps are tailored for the integration exercises contained in the next sections, so the naming conventions should be followed closely:

18. ___ You will use TSM commands (instead of the web administration GUI) to configure the server. From the management console, expand **Tivoli Storage Manager | <machine name> | TSM Server1 | Reports** and then select **Command Line**. On the right window pane, select the link labelled Command Line Prompt. The command prompt window will appear (see Figure 10-2). Commands will be entered in this window, and the results will be shown in the TSM Management Console window.

19. ___ Create a disk storage pool named CMDISKPOOL by entering the following command in the command prompt window (see Figure 10-2).

DEFINE STGPOOL CMDISKPOOL DISK DESCRIPTION=’Content Manager Storage Pool’



DEFINE STGPOOL CMDISKPOOL DISK DESCRIPTION='Content Manager Storage Pool'

Figure 10-2 *TSM Command Prompt Window*

Tivoli Storage Manager

20. ___ Create a 100MB storage pool volume for the CMDISKPOOL by entering the following command:

DEFINE VOLUME CMDISKPOOL DISK1 FORMATSIZE=100 WAIT=YES

21. ___ Create a policy domain named CMDOMAIN by entering the following command:

DEFINE DOMAIN CMDOMAIN DESCRIPTION="Content Manager Policy Domain"

22. ___ Create a policy set named CMPOLICY by entering the following command:

DEFINE POLICYSET CMDOMAIN CMPOLICY DESCRIPTION="Content Manager Policy Set"

23. ___ Create a management class named CMDISK by entering the following command:

DEFINE MGMTCLASS CMDOMAIN CMPOLICY CMDISK DESCRIPTION="Content Manager Management Class"

24. ___ Create a backup copy group by entering the following command:

DEFINE COPYGROUP CMDOMAIN CMPOLICY CMDISK
DESTINATION=CMDISKPOOL VEREXISTS=1 VERDELETED=0

25. ___ Set CMDISK as the default management class for the policy set CMPOLICY by entering the following command:

```
ASSIGN DEFMGMTCLASS CMDOMAIN CMPOLICY CMDISK
```

26. ___ Validate the policy set CMPOLICY by entering the following command:

```
VALIDATE POLICYSET CMDOMAIN CMPOLICY
```

27. ___ Activate the policy set CMPOLICY by entering the following command:

```
ACTIVATE POLICYSET CMDOMAIN CMPOLICY
```

28. ___ Create a client node that the resource manager can use to logon to TSM by entering the following command:

```
REGISTER NODE cmrm password DOMAIN=CMDOMAIN
BACKDELETE=YES FORCEPWRESET=NO
```

29. ___ Exit the TSM Management Console.

At this point, you have successfully installed a Tivoli Storage Manager server. A client node (cmrm), storage pools, and policy requirements (i.e. management class) has been created for the resource manager server.

TSM Backup Client

The TSM Backup Client should be installed on the resource manager, and any workstation which needs to access the Tivoli Storage Manager server. A typical installation of the backup client includes the TSM Client APIs, which is what the resource manager requires in order to communicate with the TSM Server. The backup client can also be used to troubleshoot and/or validate your TSM Server configuration.

> **Note:** To use a TSM server that is located on another workstation, you only need to install the TSM Backup Client on the resource manager. This will automatically install the TSM Client APIs (which is what the resource manager uses to communicate with the TSM Server).

The following steps describe how to install the TSM Backup Client on your workstation:

1. ___ Insert the TSM V5.1 Server CD into your CDROM. The installation program should start automatically.

2. ___ At the Main Menu screen, choose **Install Products** and then **TSM Backup Archive Client**.

3. ___ Select **Next** at the TSM Client Welcome Screen.

4. ___ Select **Next** to accept the default destination folder of C:\Program Files\tivoli\tsm.

5. ___ Choose to perform a typical install and select **Next** to continue.

6. ___ Select **Install** to begin the file copy process.

7. ___ Select **Finish** the complete the server initialization wizard.

At this point, the TSM Backup Archive client has also been installed on your workstation. By using the client to backup a file, you can test the TSM Server configuration. For a more in depth discussion of how you would use the client to troubleshoot integration problems, please refer to the troubleshooting section at the end of this chapter. The exercises in the following sections will demonstrate how to integrate a resource manager with the TSM server you have configured.

Integrating TSM

The resource manager uses the TSM Client APIs to access the TSM server, and can be thought of as a TSM client. As Figure 10-3 depicts, the resource manager and TSM server need not be on the same workstation. However, even if both servers existed on the same workstation, the TSM Client APIs would still be needed. In the example depicted in Figure 10-3, the resource manager stores documents on two file system volumes (C: and D:). Objects that should be stored on either the optical jukebox and / or a tape drive are sent to the TSM server. (Of course, you can use any other storage device supported by TSM.) You can also leverage the full functionality of the TSM server. For example, the TSM server can be configured so that objects are stored on optical platters, and also copied onto tapes for offsite storage.

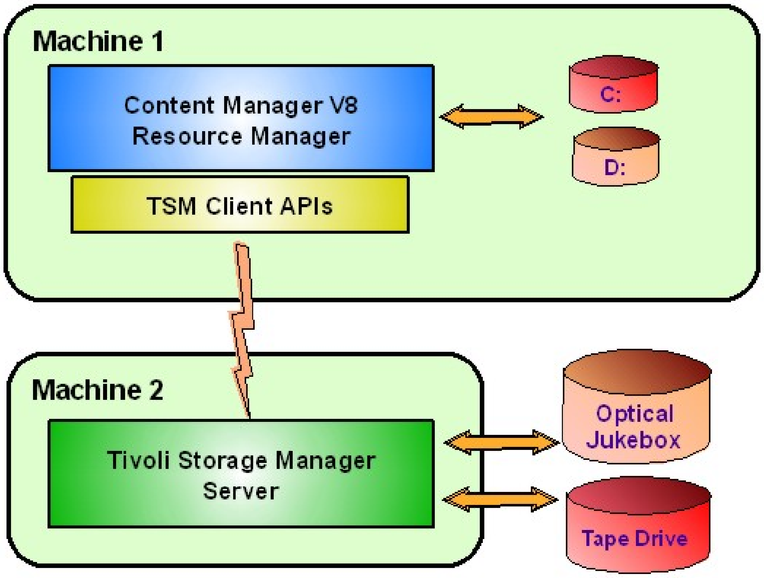

Machine 1
Content Manager V8 Resource Manager
TSM Client APIs
C:
D:
Machine 2
Tivoli Storage Manager Server
Optical Jukebox
Tape Drive

Figure 10-3 *Resource Manager and TSM Integration*

8.1 **Note:** TSM is required if you want documents in your Content Management system to be stored on storage devices other than hard disks.

When integrating Content Manager resource manager with a TSM server, you need to know three things (which can be provided by the TSM administrator):

- TSM server name
- Client node name and password to use when connecting to TSM
- Management class to be used when storing documents in TSM

The integration between the two servers is actually quite simple. You must first create a client option file which the TSM Client APIs can use to obtain configuration information. The information needed by the resource manager to access the TSM Client APIs are then specified in the icmrm.properties file. Once these two configuration files have been updated, the Content Manager System Administration Client can be used to define the TSM server and a collection which uses the TSM server for storage.

In the following sections, you will learn about each of these configuration steps. You will also learn how to test and troubleshoot the resource manager and TSM server integration.

TSM API Client Option File

The TSM API client option file contains the configuration information needed by the TSM Client APIs to access TSM servers. The TSM server name, its port, the protocol to be used to communicate with the server, and the nodename to use when connecting to the TSM server are only a few examples of what is contained in the client option file.

Your workstation can contain more than one client option file. For example, in some situations, a workstation may have both the resource manager server and the TSM Backup Archive Client installed on it. The resource manager would most likely be configured to communicate with a TSM server dedicated for Content Manager, while the TSM Backup Archive Client would be configured to backup workstation files to the company's central TSM server. In this circumstance, you would create a client option file tailored for the resource manager and another client option file tailored for the TSM backup client.

Note: Although the client option file can be named anything, traditionally, it has been referred to as dsm.opt.

Sample client option files tailored for a CM/TSM integration can be found in Chapter 17 of the publication entitled *Planning and Installing Your Content Management System* (GC27-1332). Also, a full description of all possible options can be found in the Tivoli Storage Manager Administration Guide.

In order to complete the integration exercise in this chapter, you should complete the following step:

1. ___ Create a new text file called icmrmdsm.opt, and save it in C:\Program Files\Tivoli\TSM. The text file should contain the following:

```
* Uncomment the next two lines to perform a TSM client trace
*TRACEFL INSTR_CLIENT_DETAIL  FS  API  PID  COMM  SESSION
*TRACEFIL  C:\Program Files\IBM\CM81\logs\TSM.log

* Communicate with TSM server via tcpip
commmethod  tcpip

* Specify hostname of TSM server
TCPServeraddress  localhost

* Specify TSM server port
tcpport  1500

* Specify management class
Include  ?:CMDISK*CMDISK

* Nodename to use when connecting to TSM server
NODEname  cmrm

* Authentication mode to use when connecting to TSM server
PasswordAccess Prompt
```

Note: Be careful not to make any typos when creating this file, as any syntax error will invalidate the entire client option file.

This client option file will be used when you integrate the resource manager with the TSM server, and represents the most commonly used options. Lines which begin with an asterisk are comments. Notice that the TRACEFL and TRACEFIL parameters are commented out. These two lines can be used to trace the communication between the resource manager and the TSM server, and is a useful tool for debugging integration problems. The management class and TSM client nodename to be used by the resource manager are specified by the include and nodename parameters respectively. In Content Manager version 8.1, the recommended client authentication mode is prompt. (In previous versions of Content Manager, generate was the preferred value.)

Resource Manager Properties File

The TSM Client APIs (which are used by the resource manager to access TSM) rely on variables in order to determine which option file to use and where to locate required TSM libraries. (Remember, you can have more than one client option file on a system.) These variables are defined in the resource manager properties file, which is read by the resource manager when is starts.

Note: In Content Manager version 7.1, these variables were defined in the Windows registry. In Content Manager version 8.1, these variables are defined in the icmrm.properties file.

In order to complete the integration exercise in this chapter, you should complete the following steps:

1. ___ Open `C:\WebSphere\AppServer\installedApps\icmrm.ear\icmrm.war\WEBINF\classes\com\ibm\mm\icmrm\icmrm.properties` in Notepad. (*Note: no spaces in the path.*)

2. ___ In the icmrm.properties file, update the variable values according to Table 10-1:

   The DSMI_DIR variable specifies the location of the TSM messaging API file called dscameng.txt. The DSMI_CONFIG variable points to the TSM API options file. The DSMI_LOG variable points to the TSM API log file.

Table 10-1 *TSM API Variables*

DSMI_DIR	C\:\\Program Files\\Tivoli\\tsm\\api
DSMI_CONFIG	`C\:\\Program Files\\Tivoli\\tsm\\icmrmdsm.opt` (*Note: no spaces in the path.*)

Table 10-1 *TSM API Variables*

DSMI_LOG	`C\:\\Program Files\\IBM\\CM81\\logs\\tsmapi.log` (*Note: no spaces in the path.*)

Be very careful not to alter any other section of the icmrm.properties file as doing so may prevent the resource manager from operating properly.

3. ___ Save and close icmrm.properties.

4. ___ In order for the new values to become effective, you must restart the resource manager. Stop WebSphere by running **C:\WebSphere\AppServer\bin\stopserver.bat**. You can then start it again by running C:\WebSphere\AppServer\bin\startserver.bat.

At this point the resource manager should be able to use the TSM Client APIs to communicate with the TSM server. The resource manager properties file (icmrm.properties) has been configured to point to the correct TSM client option file. The TSM client option file contains the parameters needed by the TSM APIs to communicate with the TSM server.

SMS Configuration

Once the TSM client option file and the resource manager properties file have been configured, you can use the Content Manager System Administration client to define the TSM server to the resource manager and to create a collection that utilizes the TSM server for storage.

In the following exercise, you will define the TSM server to the resource manager and create a collection for a TSM volume. The collection will use a migration policy that stores documents on Drive_C for one day before migrating them to TSM.

1. ___ Start the **System Administration** client and logon using the default user ID: ***icmadmin*** and password: ***password***.

2. ___ Expand Resource Managers | RMDB. At this point, the System Administration client will initiate a SSL connection (via https://) between itself and the Resource Manager. (If you get an error message, SSL is not configured properly.) Notice the resource manager entities that are available for configuration (see Figure 10-4).

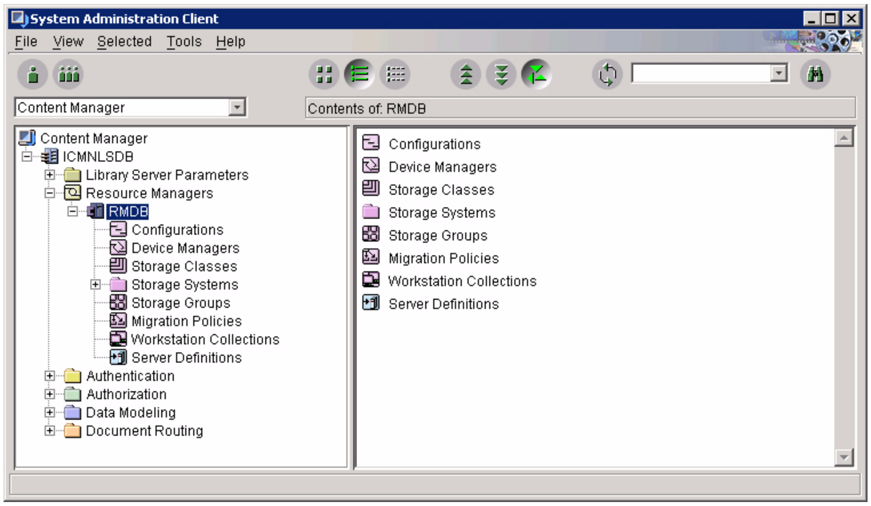
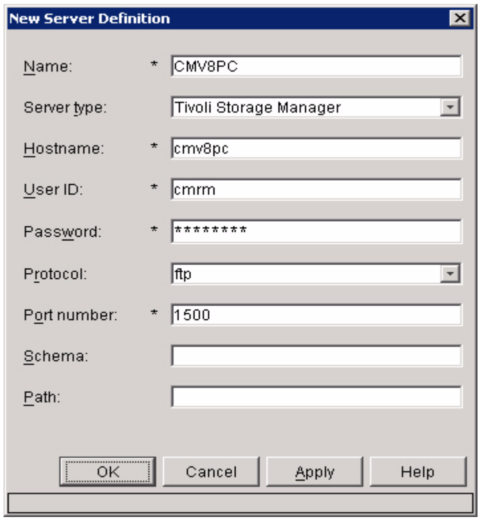


Figure 10-4 *Resource Manager SMS Configuration*

3. ___ Define a TSM server by right-clicking on **Server Definitions** and selecting **New**. The *New Server Definition* window will appear (Figure 10-5).


New Server Definition

Name: * CMV8PC

Server type: Tivoli Storage Manager

Hostname: * cmv8pc

User ID: * cmrm

Password: * ********

Protocol: ftp

Port number: * 1500

Schema:

Path:

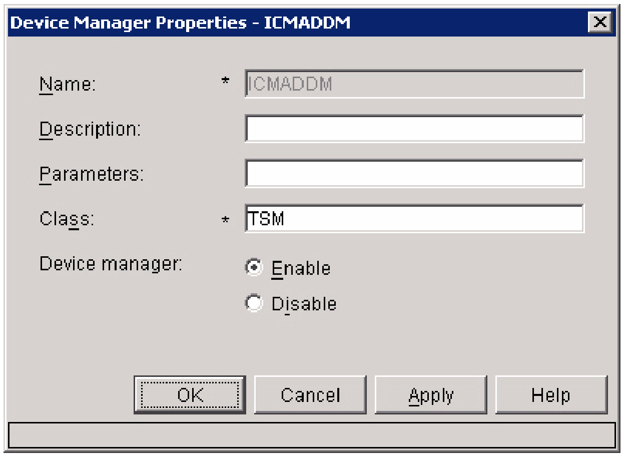
Figure 10-5 *New Tivoli Storage Manager Server Definition*

4. ___ Specify the values in Table 10-2 and then select **OK** to save the Tivoli Storage Manager server definition:

Table 10-2 *Tivoli Storage Manager Server Definition*

Name	<hostname of you machine>
Server Type	Tivoli Storage Manager
Hostname	<hostname of your machine>
Userid	cmrm
Password	password
Protocol	ftp
Port	1500 (Anything will work, as this value is ignored. The real port is specified in the TSM client option file.)
Schema	
Path	

5. ___ The TSM device manager must be enabled. Right-click on **ICMADDM** (found in the Device Managers folder) and choose **properties**. Choose **Enable** and select **OK** to save (see Figure 10-6).



Device Manager Properties - ICMADDM

Name: * ICMADDM

Description:

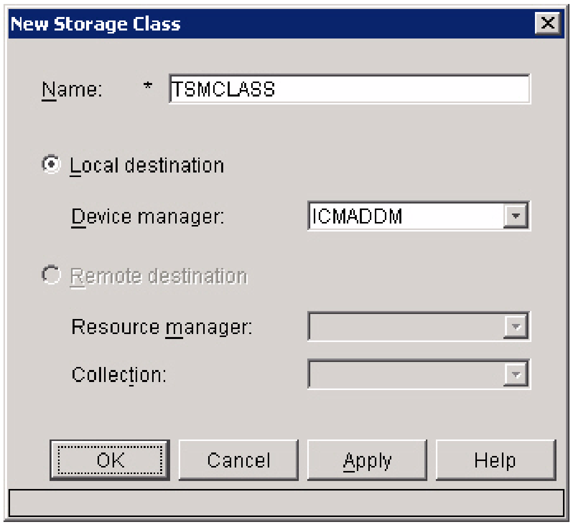
Parameters:

Class: * TSM

Device manager: ● Enable ○ Disable

Figure 10-6 *Enabling TSM Device Manager*

6. ___ Define a new storage class by right-clicking on **Storage Classes** and selecting **New**. The *New Storage Class* window will appear (Figure 10-7).



New Storage Class

Name: * TSMCLASS

● Local destination

Device manager: ICMADDM

○ Remote destination

Resource manager:

Collection:

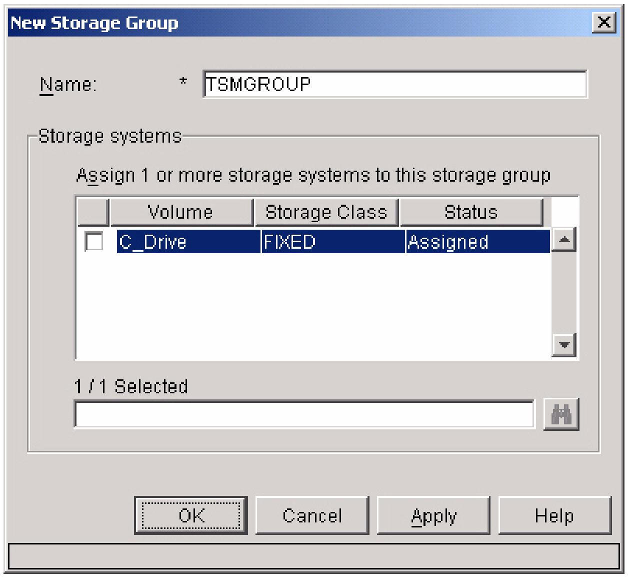
Figure 10-7 *New Storage Class Window*

7. ___ Specify the values in Table 10-3 and then select **OK** to save the storage class definition:

Table 10-3 *Storage Class Definition*

Name	TSMCLASS
Device Manager	ICMADDM

8. ___ Define a new storage group by right-clicking on **Storage Groups** and selecting **New**. The *New Storage Group* window will appear (see Figure 10-8). Name this storage group “TSMGROUP” and select **OK** to save (do NOT select any storage systems at this time).



New Storage Group

Name: * TSMGROUP

Storage systems

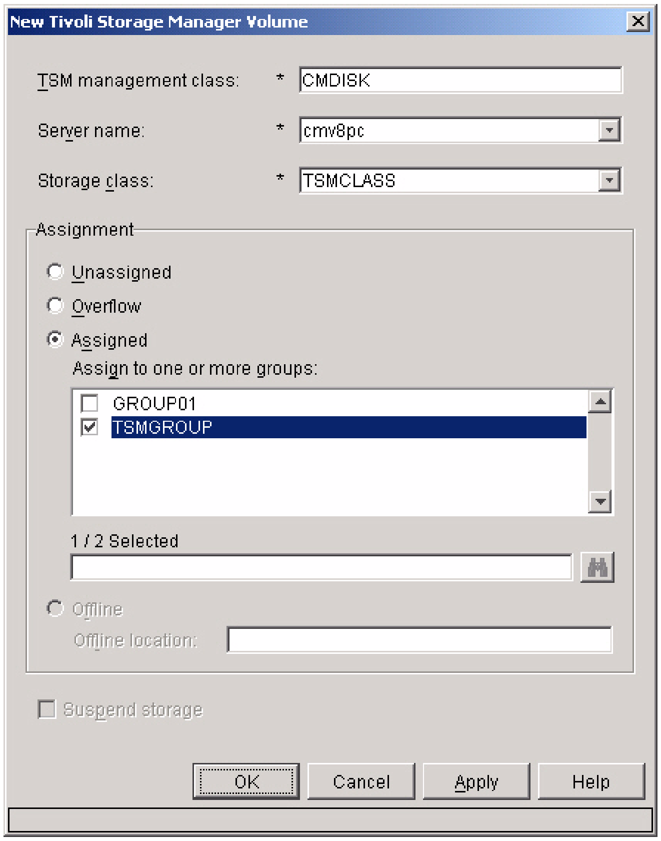
Assign 1 or more storage systems to this storage group

	Volume	Storage Class	Status
□	C_Drive	FIXED	Assigned

1 / 1 Selected

Figure 10-8 *New Storage Group Window*

9. ___ Expand the **Storage Systems** folder. Define a new TSM volume by right-clicking on **Tivoli Storage Manager volumes** folder and choose **New**. The *New Tivoli Storage Manager Volume* window will appear (Figure 10-9).


New Tivoli Storage Manager Volume

TSM management class: * CMDISK

Server name: * cmv8pc

Storage class: * TSMCLASS

Assignment

○ Unassigned

○ Overflow

● Assigned

Assign to one or more groups:

□ GROUP01

☑ TSMGROUP

1 / 2 Selected

○ Offline

Offline location:

□ Suspend storage

Figure 10-9 *New Tivoli Storage Manager Volume*

10. ___ Specify the values in Table 10-4 and then select **OK** to save the volume definition:

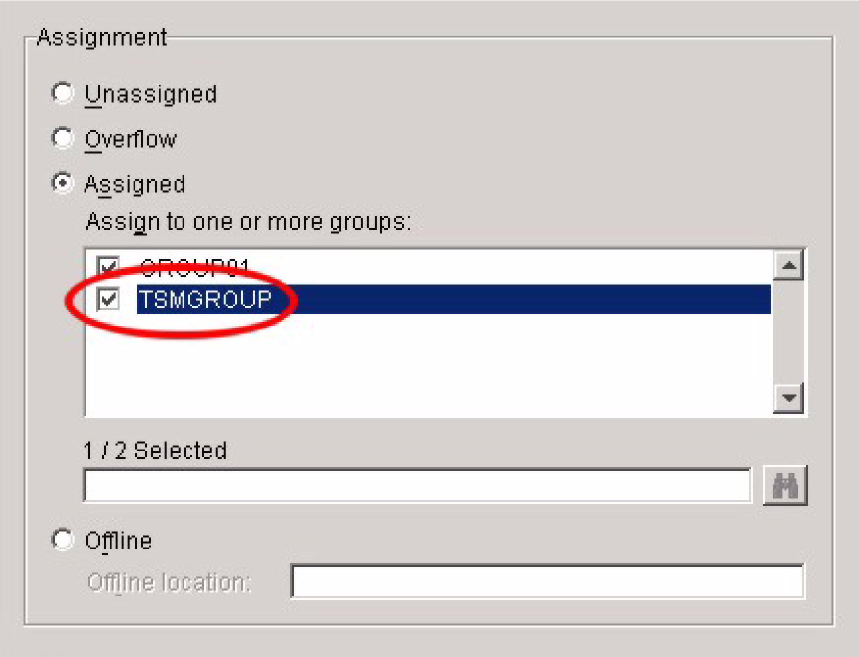
Table 10-4 *Tivoli Storage Manager Volume Definition*

TSM management class	CMDISK
Server name	<hostname of your workstation>
Storage class	TSMCLASS
Assignment	Assigned, AND select TSMGROUP

8.1

Note: The Content Manager TSM volume maps directly to a TSM management class. If you type an invalid management class name, then object migration will fail.

11. ___ Right-click on **C_Drive** (found under Storage Systems | File System Volumes) and choose **properties**. Add an additional assignment by placing a checkmark next to the group named TSMGROUP (see Figure 10-10). Be careful NOT to remove any of the current assignments. Select **OK** to save the new assignment.



Assignment

○ Unassigned

○ Overflow

● Assigned

Assign to one or more groups:

☑ GROUP01

☑ TSMGROUP

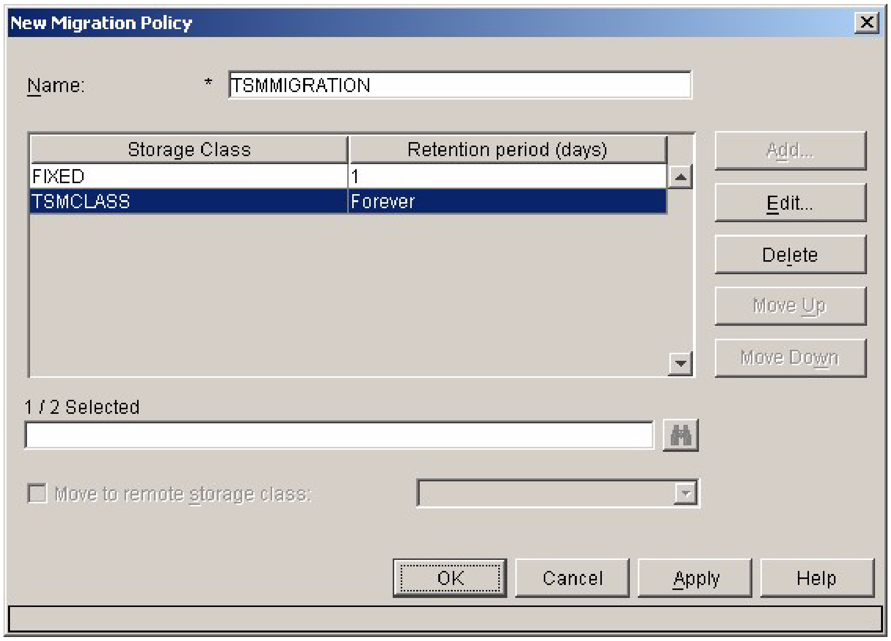
1 / 2 Selected

○ Offline

Offline location:

Figure 10-10 *Assigning C_Drive to the TSMGROUP*

12. ___ Define a new migration policy by right-clicking on **Migration Policies** and selecting **New**. The *New Migration Policy* window will appear (see Fig. 10-11 on page 321).



Name: * TSMMIGRATION

Storage Class	Retention period (days)
FIXED	1
TSMCLASS	Forever

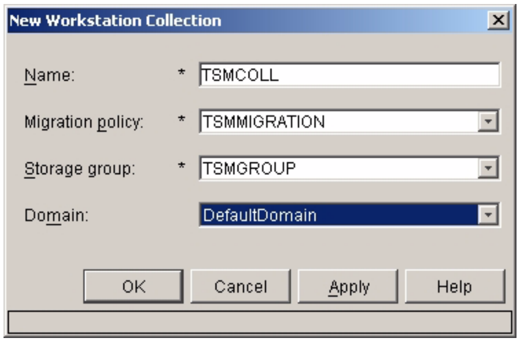
1 / 2 Selected

□ Move to remote storage class:

Figure 10-11 *New Migration Policy Window*

13. ___ Name this migration policy **TSMMIGRATION**. Select **Add** to specify the first migration step. Choose **FIXED**, and select **1 day** as the retention period. Select **Add** again to specify the second migration step. Choose **TSMCLASS**, and select **FOREVER** as the retention period. Press **OK** to save this migration policy.

14. ___ Define a new collection by right-clicking on **Workstation Collections** and selecting **New**. The *New Workstation Collection* window will appear (see Figure 10-12).



Name: * TSMCOLL

Migration policy: * TSMMIGRATION

Storage group: * TSMGROUP

Domain: DefaultDomain

Figure 10-12 *New Workstation Collection Window*

15. ___ Specify the values in Table 10-5 and then select **OK** to save the workstation collection definition:

Table 10-5 *Workstation Collection Definition*

Name	TSMCOLL
Migration policy	TSMMIGRATION
Storage group	TSMGROUP
Domain	DefaultDomain

At this point, Tivoli Storage Manager has been integrated with your resource manager. Any documents which use the TSMCOLL collection will be migrated to TSM after 30 days. In the next section, you will test the integration by creating an item type which uses the TSMCOLL collection.

Using TSM for Storage

The integration between the resource manager and Tivoli Storage Manager can easily be tested by creating an item type which uses the TSMCOLL you previously defined during the object storage configuration exercise. In the following exercises, you will learn how to determine if a document has been migrated from the resource manager to the TSM server. By validating the integration, you can be sure that the documents in your Content Management system will be in their proper storage location.

Create Item Type that Uses TSM Collection

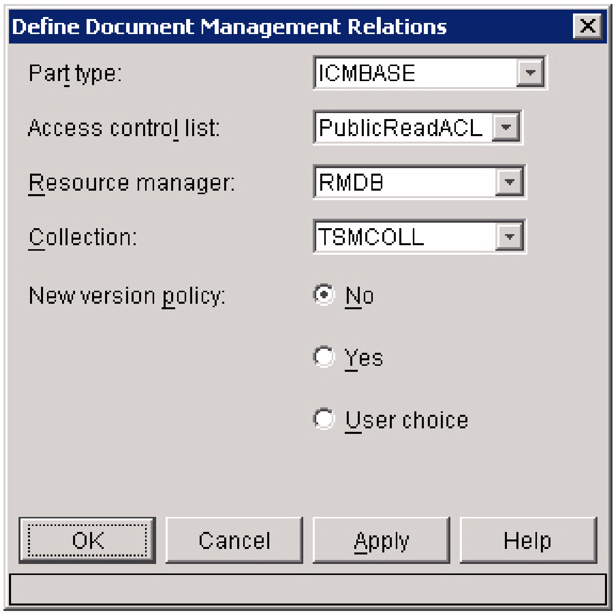
In the following exercise, you will create an item type that uses the TSM collection you previously defined. As this item type will only be used for testing, other features such as text search or child components will not be used.

1. ___ Create a new item type by right-clicking on **Item Types** (located under the Data Modeling folder) and selecting **New**.

2. ___ On the Definition page, type **TSMTest** in the Name field. Leave all other option on this page at their default values.

3. ___ On the Attributes page, add only the attribute named **USER_ID**. Leave the options for this attribute at their default values.

4. ___ On the Document Management page, select the **Add** button. The Define Document Relations window will appear (see Figure 10-13).



Define Document Management Relations

Part type: ICMBASE

Access control list: PublicReadACL

Resource manager: RMDB

Collection: TSMCOLL

New version policy: ● No ○ Yes ○ User choice

Figure 10-13 *Define Document Management Relations Window*

5. ___ Specify the values in Table 10-6 and then select **OK** to save the item type definition:

Table 10-6 *Document Management Relations Definition*

Part type	ICMBASE
Access control list	PublicReadACL
Resource manager	RMDB
Collection	TSMCOLL
New version policy	No

You should be aware that because the ICMANNOTATION, ICMNOTELOG, and ICMBASETEXT part types were not added; annotations, notelogs, and textsearch will not be supported by this item type. As this item type will be used only to test the migration of an image from DriveC to TSM, only the ICMBASE part type is needed.

Test Migration of Objects to TSM

The TSMTest item type that you created will be used to test the migration of objects to TSM. This item type uses the TSMCOLL collection, which is configured to store new documents on Drive C for one day before migrating them to TSM forever. You will import an image into this item type, alter the system date, and then start the migrator process. Once the migrator process is complete, the contents of the TSM volume will be queried in order to validate the migration.

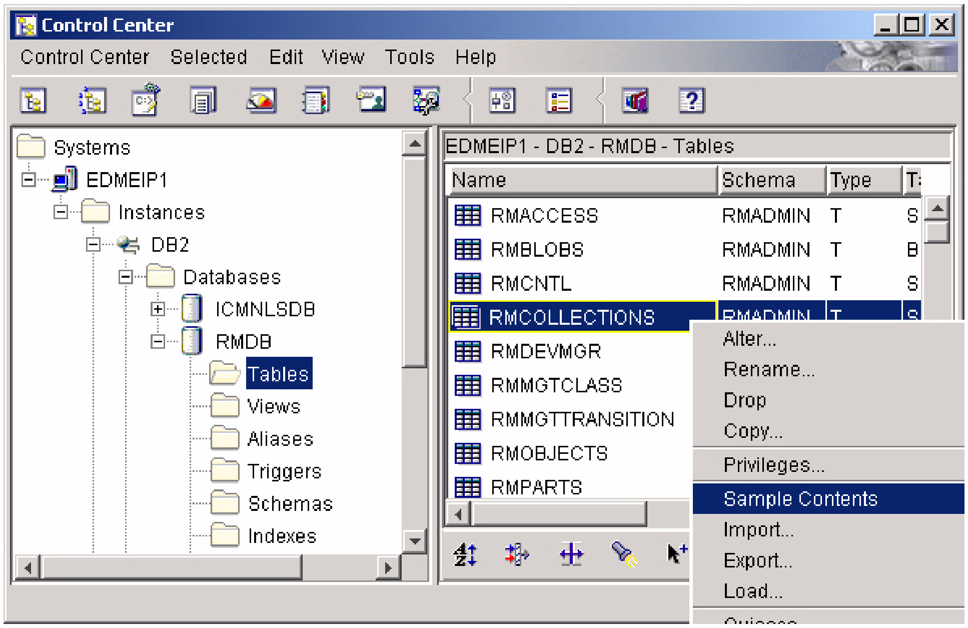
The following exercise will walk you through the process of importing and tracking a document as it is migrated according to the migration policy:

1. ___ Use the Content Manager Windows Client to import two documents into the **TSMTest** item type. (In order to keep the test manageable, do not import more than two documents.)

2. ___ To verify that the import was successful, search for and view the documents you just imported.

3. ___ Documents stored on file system volumes will be placed in a directory named lbosdata. To verify this, go to C:\lbosdata. Notice there are subdirectories (i.e. 00001 and 00002). Each directory represents a collection.

4. ___ To determine which collection each directory corresponds to, open the DB2 Control Center (**Start | Programs | IBM DB2** | **Control Center**) and go the RMDB tables folder (expand system name | **Instances | DB2 | Databases | RMDB | Tables**). Right-click on the table named **RMCOLLECTIONS** and choose **Sample Contents** from the popup menu (see Figure 10-14).



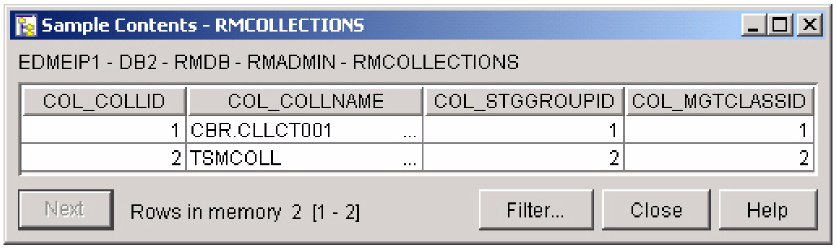
EDMEIP1 - DB2 - RMDB - Tables

Name	Schema	Type	T:
RMACCESS	RMADMIN	T	S
RMBLOBS	RMADMIN	T	B
RMCNTL	RMADMIN	T	S
RMCOLLECTIONS	RMADMIN	T	S
RMDEVMGR			
RMMGTCLASS			
RMMGTTRANSITION			
RMOBJECTS			
RMPARTS			

Figure 10-14 *Viewing Sample Contents of a Table*

> **Note:** DB2 Control Center will show the sample contents of a table. This means that for larger tables, all rows may not necessarily be displayed.

5. ___ The RMCOLLECTIONS table will appear (see Figure 10-15). In this case, the 00001 subdirectory represents the CBR.CLLCT001 collection, and 00002 subdirectory represents the TSMCOLL collection. **Close** the RMCOLLECTIONS sample contents window.



EDMEIP1 - DB2 - RMDB - RMADMIN - RMCOLLECTIONS

COL_COLLID	COL_COLLNAME	COL_STGGROUPID	COL_MGTCLASSID
1	CBR.CLLCT001 ...	1	1
2	TSMCOLL ...	2	2

Rows in memory 2 [1 - 2]

Figure 10-15 *Resource Manager Collections*

6. ___ Go into the subdirectory for the TSMCOLL collection (i.e.

C:\lbosdata\00002). There should be one or more subdirectories named by a two digit number (i.e. "01", "35"). These subdirectories are referred to as *numbuckets*. Due to limits of the file system, it may not be possible to store all document files in a single directory (as your system may have over 1 million documents). The number of numbuckets assigned to a particular file system volume can be updated via the System Administration Client (right-click on the volume, and choose properties). For example, if the numbuckets for this volume (C_Drive) were set to 3, then you would eventually see three subdirectories. Files would get placed in each directory in a round-robin fashion.

7. ___ Go into the numbucket subdirectory (i.e. C:\lbosdata\00002\01). The documents you just imported into the **TSMTest** item type should be in this directory. Notice that the filenames are different (but the actual file contents have NOT been changed).

> **Note:** Never delete files from the lbosdata directory. If you do, the library server and resource manager databases will contain rows for documents that do not physically exists.

8. ___ Now that you have verified that the documents are stored on the C_Drive volume, you are ready to start the migration of the documents to TSM. Before doing so, use the DB2 Control Center to view the RMOBJECTS table. All documents managed by this resource manager (including the ones you have imported into the TSMTest item type) should be found in this table. Notice the rows which have OBJ_COLLECTIONID set to the TSMCOLL ID (which, in this example, is two).

   ___ Notice that the documents stored in the TSMCOLL currently has an OBJ_VOLUMEID of 1. To determine which storage volume corresponds with an ID of 1, check the RMVOLUMES table.

   ___ Observe the OBJ_ACTIONDATE column. When the migrator process starts, it runs a query against this table, and looks for every item / row with an OBJ_ACTIONDATE less than or equal to the current system date. This is how the migrator determines which documents are candidates for migration.

   ___ Notice that the documents in the TSMCOLL collection have an actiondate of tomorrow. In order to get the migrator process to migrate these documents, you must change the SYSTEM date to be greater than or equal to the actiondate. Once the documents have been migrated to

TSM, their actiondate will be updated to **9999-12-31** (which represents FOREVER).

9. ___ Increase the SYSTEM date by 1 day. The system date should now match the actiondate value in the RMOBJECTS table.

8.1 **Note:** At the end of this exercise, be sure you restore the system date to its original setting.

10. ___ Go to the *Windows Services Control* Panel, and start the service named **ICM Migrator (RMDB)**. At this point, the migrator process will start. The first thing it will do is check for documents that are candidates for migration (by running a query against the RMOBJECTS table and looking for rows with an actiondate less than or equal to the current date).

    Once lists of documents are built, the migrator will create a thread to handle each volume in the system. This is a new feature of version 8.1. Previously, a single thread handled all document migration. With version 8.1, multiple document migrations can take place concurrently.

11. ___ After a few seconds, recheck the **RMOBJECTS** table. Documents in the TSMCOLL collection should now have an actiondate value of 9999-12-31 (since this was the last migration step). Also notice the new value in the OBJ_VOLUMEID column.

8.1 **Note:** If the documents failed to migrate, refer to the last section of this chapter for troubleshooting tips.

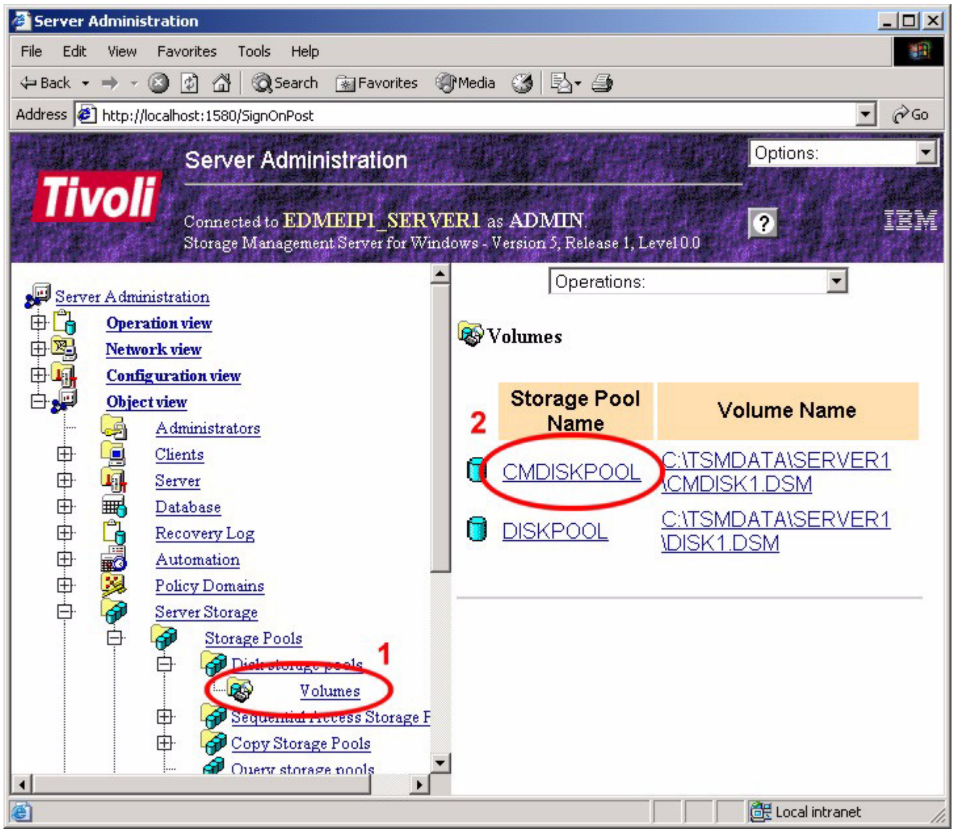
12. ___ Take a look at the *C:\lbosdata\00002\01* directory. Notice that the two files no longer exist there (they are now stored in the TSM server).

13. ___ Use the Content Manager Windows client to search for AND view these documents. After viewing the documents, look at the C:\Staging directory. The resource manager server uses this directory as a cache. When a client requests a document that is stored in TSM, the resource manager server will retrieve the document from TSM, store the document in the C:\staging directory, and then deliver the document to the client. The reason this caching is necessary is because documents stored in TSM are usually placed on much slower devices (such as tape or optical jukeboxes). By temporarily placing requested documents in the C:\staging directory, any future requests for this particular document will be extremely quick. (The purger process periodically cleans up the C:\Staging directory.)

14. ___ To be absolutely certain that the documents are indeed stored within TSM, you can use the TSM Administrator's Console to view the contents of your TSM volumes. Start the TSM Administrator's console by opening a web browser and going to http://localhost:1580.

15. ___ Login as **admin**. The default password for this user ID is **admin**.

16. ___ On the left frame, expand **Object view | Server Storage | Storage Pools | Disk storage pools | Volumes.** Select on the **CMDISKPOOL** link (see Figure 10-16).



Connected to EDMEIP1_SERVER1 as ADMIN.
Storage Management Server for Windows - Version 5, Release 1, Level 0.0

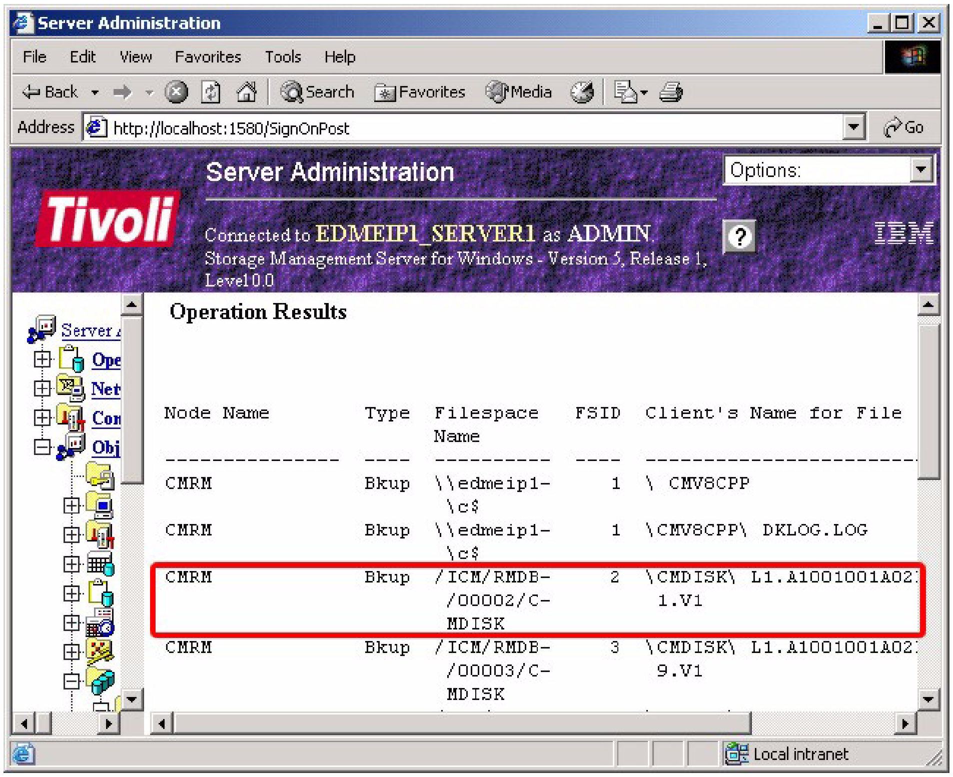
Volumes

Storage Pool Name	Volume Name
CMDISKPOOL	C:\TSMDATA\SERVER1\CMDISK1.DSM
DISKPOOL	C:\TSMDATA\SERVER1\DISK1.DSM

Figure 10-16 *Retrieving Properties of a TSM Volume*

17. ___ From the combo box on the top of the screen, select the **Query contents of a storage pool volume** option. A query form will appear. Select the **Finish** button to accept the default search values.

A report similar to that of Figure 10-17 will be displayed. The *Filespace Name* column tells you which files the resource manager owns. The last column shows the actual resource manager filename.


Server Administration
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:1580/SignOnPost
Go
Server Administration
Options:
Tivoli
IBM
Server
Ope
Net
Con
Obj
Local intranet

Connected to EDMEIP1_SERVER1 as ADMIN.
Storage Management Server for Windows - Version 5, Release 1, Level 0.0

Operation Results

```
Node Name          Type  Filespace   FSID  Client's Name for File
                         Name
----------------   ----  ----------  ----  ------------------------
CMRM               Bkup  \\edmeip1-     1  \ CMV8CPP
                          \c$
CMRM               Bkup  \\edmeip1-     1  \CMV8CPP\ DKLOG.LOG
                          \c$
CMRM               Bkup  /ICM/RMDB-     2  \CMDISK\ L1.A1001001A02
                          /00002/C-         1.V1
                          MDISK
CMRM               Bkup  /ICM/RMDB-     3  \CMDISK\ L1.A1001001A02
                          /00003/C-         9.V1
                          MDISK
```

Figure 10-17 *Content Manager Files Stored in a TSM Volume*

18. ___ Close the TSM Administrator Console. Take some time now to browse through the remaining resource manager tables. Also, take a closer look at the RMOBJECTS table and see what other information is stored there. When finished browsing the tables, close the DB2 Control Center.

At this point, you have successfully integrated the resource manager with TSM. The RMOBJECTS table and the TSM Admin Console proved invaluable in determining the physical location of documents. The concepts learned can also be applied to configurations which have the resource manager and TSM server on separate workstations. In the next section, you will learn how to troubleshoot integration problems.

Troubleshooting TSM Integration

In this section, you will be introduced to various resources for troubleshooting problems with a TSM integration. By utilizing log files, traces, and the TSM Backup Archive client, you can quickly and easily resolve almost any configuration error. The following resources will be discussed:

- Resource manager migrator log
- TSM API log
- TSM Backup Archive Client

Resource Manager Migrator Log

The resource manager server contains a logging facility based upon the open source Log4J project. A detailed description of this logging facility and the various logging options can be found in Chapter 15. The logging control file for the migrator process is named icmrm_migrator_logging.xml. This file is located, by default, in C:\WebSphere\AppServer\installedApps\icmrm.ear\icmrm.war.

To trace the migrator process, open icmrm_migrator_logging.xml in Notepad, and locate the following two lines (towards the end of the file):

```
<priority value="INFO" class="com.ibm.mm.icmrm.util.ICMRMPriority"/
>
<appender-ref ref="ASYNC"/>
```

To obtain detailed debugging information, change the priority value from INFO to DEBUG (refer to Chapter 15 for a description of other valid priority values). To send log messages to a file, change the appender-ref value from ASYNC to FILE. Restart the resource manager web application and migrator process. Detailed messages concerning the migration of documents will be logged in a file named icmrm.migrator.logfile. This file is located, by default, in C:\WebSphere\AppServer\logs.

TSM Client API Log

While the resource manager logging facility is useful in determining that a problem does exists, it may not always be the most helpful in telling you the exact details of what is causing the problem. For example, in certain situations, the resource manager logs may only contain information alluding to a connection problem with the TSM server. Details on what is causing the connection problem may not necessarily be in the resource manager log files.

Recall that the resource manager (and its processes) use the TSM Client APIs to communicate with the TSM server. By default, when an error occurs, the TSM Client APIs will log the error information in a file named dsierror.log. The information contained in this file proves invaluable in locating and resolving problems which deal solely with TSM, and have nothing to do with the resource manager configuration. Errors such as expired passwords and invalid management class names will be logged in this file.

Note: When troubleshooting a Tivoli Storage Manager integration problem, the **dsierror.log** file usually contains the cause of the error.

One common error which you may see in the dsierror.log file is that the dsm.opt file cannot be located. Recall that the TSM Client APIs use the DSMI_CONFIG variable to determine which option file to use. The exercises in this chapter instructed you to set DSMI_CONFIG to icmrmdsm.opt. If there is a syntax error in the option file you specified (icmrmdsm.opt), or if the file cannot be opened, then the TSM Client APIs will fallback to using the default option filename of dsm.opt. Therefore, this type of error message indicates that you probably have a typo in the icmrmdsm.opt file.

TSM Backup Archive Client

In some situations, the resource manager and TSM Client API log files may indicate that an invalid TSM Server configuration is keeping documents from being migrated. One of the easiest ways to test a TSM Server configuration is to use the TSM Backup Archive Client to backup a file.

The TSM Backup Archive Client also uses a set of variables to determine which client option file to use. More specifically, the DSM_CONFIG environment is used by the TSM Backup Archive Client to determine which client option file to use. This variable should point to the client option file used by the resource manager. Doing so will ensure the backup client is using the same TSM configuration as the resource manager.

For example, to use the TSM Backup Archive Client to test the TSM configuration, the following steps can be done:

1. ___ Go to a command prompt window.
2. ___ Enter **cd c:\program files\tivoli\tsm\baclient**.
3. ___ Enter **set dsm_config=c:\program files\tivoli\tsm\icmrmdsm.opt**.

4. ___ Start the TSM Backup Archive Client by entering **dsm**.

5. ___ You will be prompted for the CMRM node name password. Enter **password** as the password.

6. ___ Backup a small text file.

If the TSM Backup Archive Client fails to backup a file, then the resource manager server will also fail. (Remember, the resource manager server does NOT archive files; it backs up files.) This indicates a problem with the TSM Server configuration. In this circumstance, you should check the TSM Server activity log to determine what the problem is.

Summary

In this chapter, you were introduced to the Tivoli Storage Manager Server and how it is integrated with Content Manager. TSM provides an automated, policy managed backup, archive, and space management facility for file servers and workstations. A wide variety of storage devices such as optical jukeboxes are supported, and also includes its own migration policy configuration (so documents can move between different storage devices within TSM). The Content Manager resource manager uses the TSM Client APIs to communicate with the TSM server. This integration allows you to store documents on storage devices other than hard disks. The storage management capabilities (i.e. copy storage pools, offsite storage) can also be leveraged by Content Manager.

The configuration values needed by the TSM Client APIs are stored in a client option file (i.e. dsm.opt), and contain information such as the TSM servername, port number, and communication method to be used. The TSM Client APIs will use the values specified by the DSMI_CONFIG, DSMI_DIR, and DSMI_LOG variables to locate the client option and TSM library files. These variables are defined in the resource manager icmrm.properties file. Once the client option and icmrm.properties files have been properly configured, the Content Manager System Administration client can be used to define the TSM server and to create a collection which uses TSM for document storage.

Lastly, you learned how to test and track the migration of documents from the resource manager to TSM. Important database tables and column values were reviewed, and steps for troubleshooting integration problems were described.

CHAPTER 11

VideoCharger Integration

- Overview
- Installation
- Configuration
- Integration

In this chapter, you will be introduced IBM VideoCharger and how it can be integrated with a Content Manager Version 8.1 system. You will learn what services are provided by a VideoCharger server and how it can be used to improve access to media objects that are managed by IBM Content Manager. Exercises contained within this chapter will walk you through the process of performing the installation, configuration, and integration of VideoCharger. The goal of this chapter is not to focus on the VideoCharger server, but on how it can be used within a Content Manager system.

Overview

IBM VideoCharger allows you to deliver video and audio files, called *asset*s, in real-time (called *streamin*g) to clients over a network. Streaming from the server eliminates the need for clients to first download the entire object before being able to view it. The media formats that a VideoCharger Version 8.1 server can stream are shown in Table 11-1.

Table 11-1 *Media Formats Which VideoCharger V8.1 Can Stream*

Media Format	File Extension	Type
MPEG-1	.MPG	Audio and/or video
MPEG-2	.MPG	Audio and/or video
Audio Video Interlaced	.AVI	Audio and/or video
H.263 + G.273 interleaved	.IBA	Audio and/or video
QuickTime (hinted)	.MOV	Audio and/or video
MP3	.MP3	Audio only
WAV	.WAV	Audio only
HotMedia	.MVR	Audio and/or video
MPEG-4	.MP4	Audio and/or video

The importance of being able to stream large media files is depicted in Figure 11-1 on page 337. In this example, both clients have requested a 100MB video from a Content Management system. When the video is streamed, the user is able to watch the video as it being downloaded to the workstation. When the video is not streamed, the user must wait for the entire video to be downloaded to the workstation before it can be viewed. Because the time is takes to download large media files is significant, the use of streaming is required in order to provide a satisfactory response time.

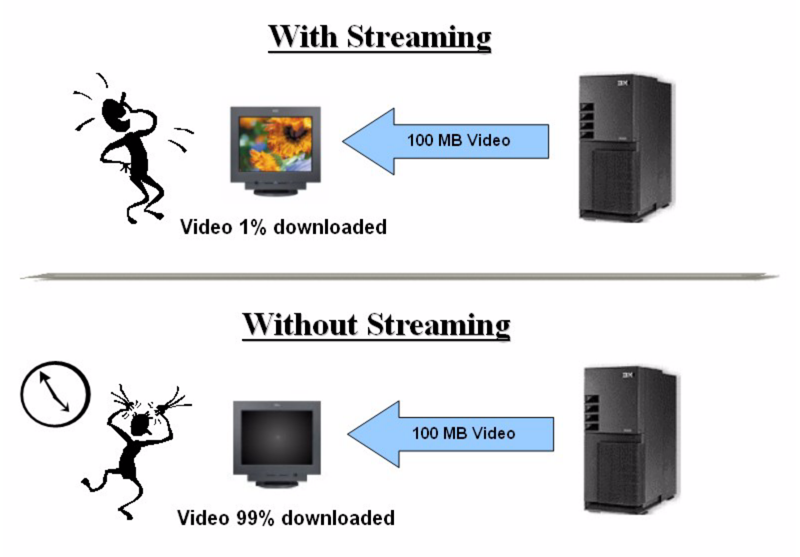


Figure 11-1 *Streaming and Non-streaming Video*

In addition to providing the capability to stream video/audio assets, VideoCharger can manage the storage of media files (which are usually quite large). However, the indexing and searching capabilities are limited. By integrating VideoCharger with a resource manager, Content Manager can manage the associated metadata while relying on VideoCharger to manage the storage and delivery of the media files. Furthermore, the access control to media objects can be managed from the Content Management system.

The integration of a VideoCharger server in a Content Manager system is depicted in Figure 11-2 on page 338. The metadata (attributes) associated with these media assets are stored in the library server database. Notice that the VideoCharger server is specifically integrated with the resource manager. The media archive server is a component of the VideoCharger system, and is used to archive large, rarely used, media files. Before a media object that is stored in the media archive server can be streamed to clients, it must first be destaged to the VideoCharger server.

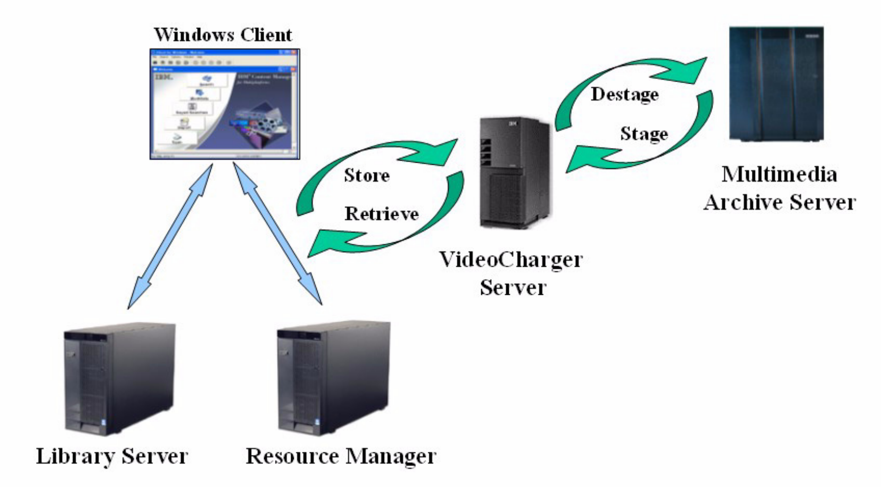


Figure 11-2 *Content Manager Integration With VideoCharger*

The following steps will occur when a Content Manager client makes a request that involves an integrated VideoCharger server:

1. ___ Client requests a media object from the library server.
2. ___ Library server returns security token and information on which resource manager to contact.
3. ___ Client requests the media object from the resource manager.
4. ___ Resource manager requests the media object from the VideoCharger Server.
5. ___ Depending on the request, the following occurs:

   Load Request

   The media object loads onto the VideoCharger Server with an asset name of:*L*x.*ABCDEFGHIJKLMNOPQRSTUVWXYZ*.*Vy* where ***x*** represents the library server number, *ABCDEFGHIJKLMNOPQRSTUVWXYZ* represents a 26-character asset name, and ***y*** represents the version control number.

   Play Request

   The VideoCharger Server sends a temporary metadata file to the client, containing system instructions on streaming the media object. The metadata files is sent to the client with a MIME type of video/x-ibm-ivs. Based on this

MIME type, the client opens the appropriate video player and initiates a streaming session with the VideoCharger Server. The VideoCharger streams the media object to the Player.

In the remainder of this chapter, you will learn how to install a VideoCharger server and integrate it with the resource manager. You will also validate this integration by importing a video and then using the clients to test the streaming function.

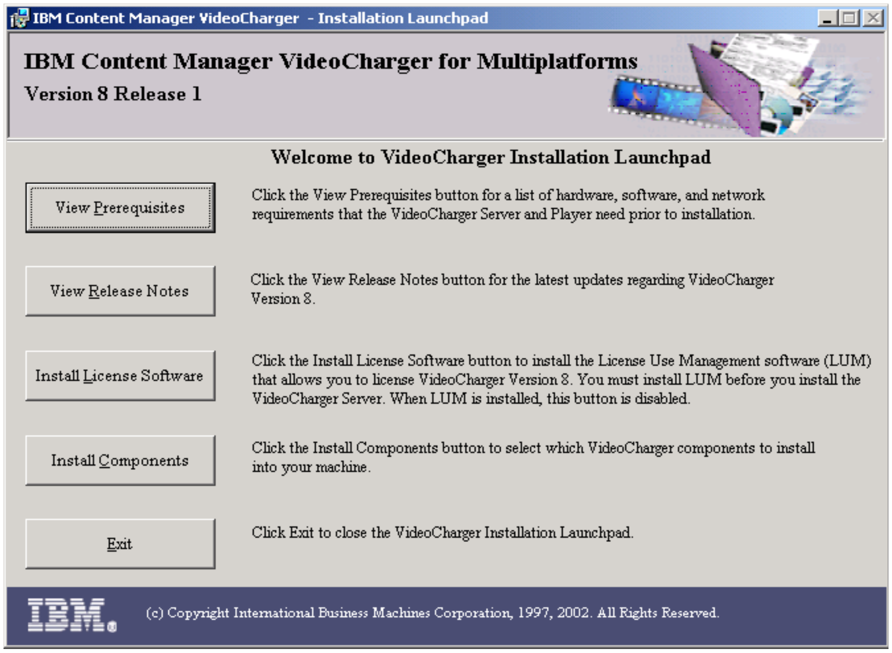
Installation

In this section you will learn how to install the VideoCharger server and player on Windows. All components will be installed using their default location and configuration. After verifying the installation, you will integrate the VideoCharger server with Content Manager.

License Use Management (LUM) Software

The VideoCharger server requires that the License Use Management (LUM) be installed. This software is used to manage the amount of concurrent streams being delivered by the VideoCharger server.

1. ___ Start the VideoCharger installation by inserting the VideoCharger CD into the CDROM drive of your workstation.
2. ___ Choose the English language for installation and select **OK**.
3. ___ Select **Install License Software** from the Welcome to *VideoCharger Installation Launchpad*, (see Figure 11-3).


IBM Content Manager VideoCharger - Installation Launchpad
IBM Content Manager VideoCharger for Multiplatforms
Version 8 Release 1
View Prerequisites
View Release Notes
Install License Software
Install Components
Exit
IBM

Welcome to VideoCharger Installation Launchpad

Click the View Prerequisites button for a list of hardware, software, and network requirements that the VideoCharger Server and Player need prior to installation.

Click the View Release Notes button for the latest updates regarding VideoCharger Version 8.

Click the Install License Software button to install the License Use Management software (LUM) that allows you to license VideoCharger Version 8. You must install LUM before you install the VideoCharger Server. When LUM is installed, this button is disabled.

Click the Install Components button to select which VideoCharger components to install into your machine.

Click Exit to close the VideoCharger Installation Launchpad.

(c) Copyright International Business Machines Corporation, 1997, 2002. All Rights Reserved.

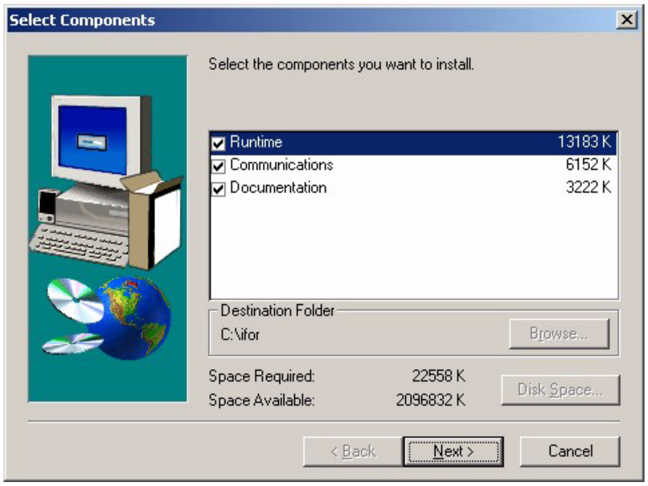
Figure 11-3 *Welcome to VideoCharger Installation Launchpad*

4. ___ From the *Welcome* window, select **Next** to continue.

5. ___ From the *Information* window, select **Next** to continue.

6. ___ Accept the default destination drive (C:) and select **Next** to continue.

7. ___ Leave all components selected and select **Next** to continue, (see Figure 11-4).



Select Components

Select the components you want to install.

☑ Runtime	13183 K
☑ Communications	6152 K
☑ Documentation	3222 K

Destination Folder
C:\ifor

Space Required: 22558 K
Space Available: 2096832 K

Figure 11-4 *Select LUM Components Window*

8. ___ Select **Finish** to complete the installation of the License Use Management software.

VideoCharger Server

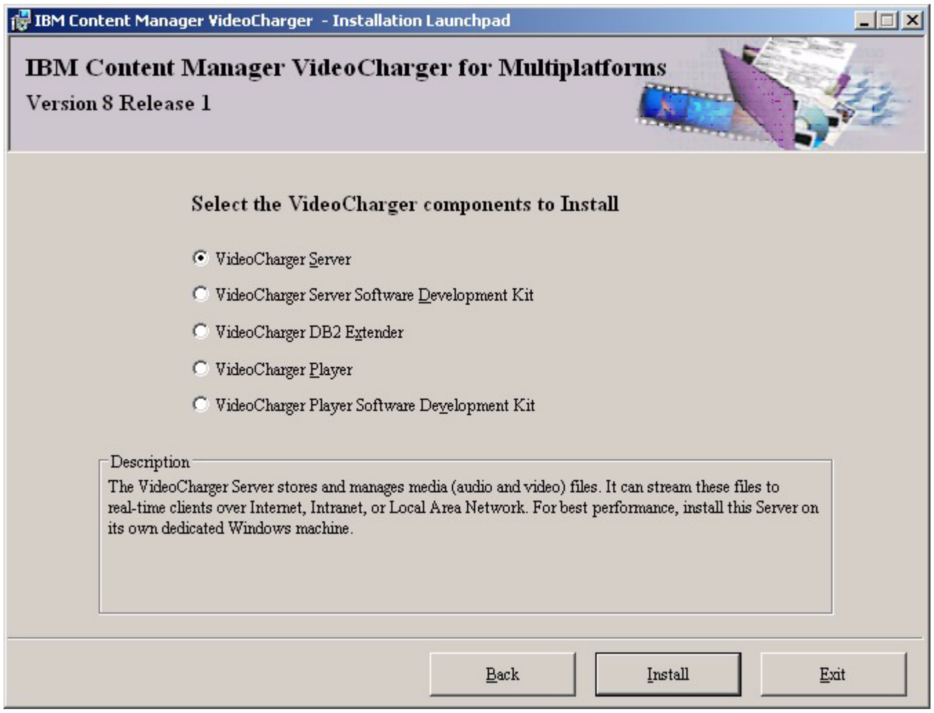
Once the License Use Management software and a supported web server have been installed, the VideoCharger installation may be started. VideoCharger will be configured to use the IBM HTTP Server (as you have already installed it from the prerequisite software installation exercise in the Chapter on *Installing Prerequisites*).

1. ___ Start the VideoCharger installation by inserting the VideoCharger CD into the CDROM drive of your workstation.

2. ___ Choose the **English** language for installation and select **OK**.

3. ___ Select **Install Components** from the *Welcome to VideoCharger Installation Launchpad*, (see Figure 11-3).

4. ___ Choose **VideoCharger Server** and select **Install**, (see Figure 11-5).


IBM Content Manager VideoCharger - Installation Launchpad
IBM Content Manager VideoCharger for Multiplatforms
Version 8 Release 1

Select the VideoCharger components to Install

● VideoCharger Server
○ VideoCharger Server Software Development Kit
○ VideoCharger DB2 Extender
○ VideoCharger Player
○ VideoCharger Player Software Development Kit

Description
The VideoCharger Server stores and manages media (audio and video) files. It can stream these files to real-time clients over Internet, Intranet, or Local Area Network. For best performance, install this Server on its own dedicated Windows machine.

Figure 11-5 *Select the VideoCharger Components*

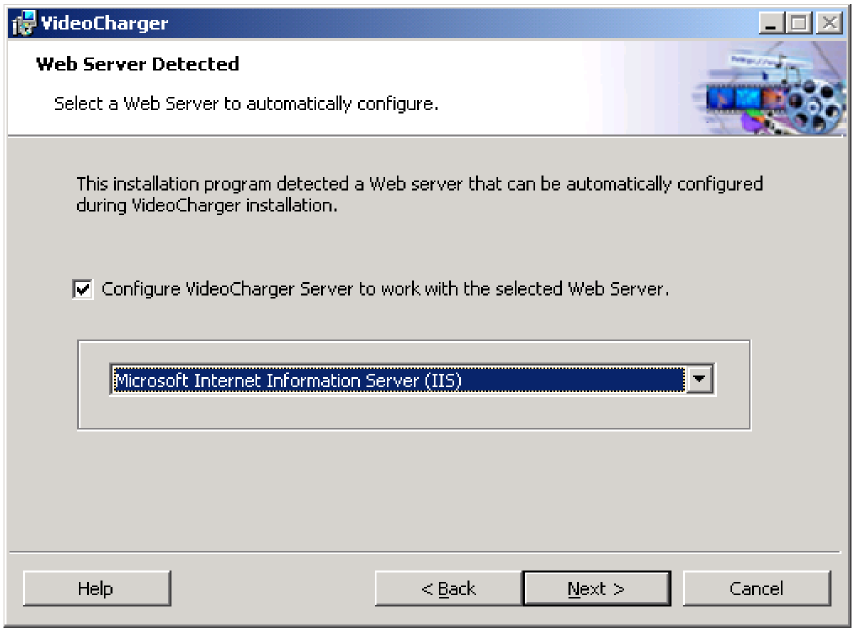
Note: You may see a warning message indicating that the web server prerequisite was not found. As the installation program did not detect the version of IBM HTTP Server you installed during the prerequisite exercises, you can safely select **Continue** to proceed with the installation.

5. ___ On *VideoCharger Server Welcome* window, select **Next** to continue.

6. ___ Accept the license agreement and select **Next**.

7. ___ Choose to perform a **Typical** install and select **Next** to continue.

8. ___ Depending on the configuration of your workstation, either one of the windows shown in Figure 11-6 or Figure 11-7 on page 344 will be displayed.



VideoCharger

Web Server Detected

Select a Web Server to automatically configure.

This installation program detected a Web server that can be automatically configured during VideoCharger installation.

☑ Configure VideoCharger Server to work with the selected Web Server.

Microsoft Internet Information Server (IIS)

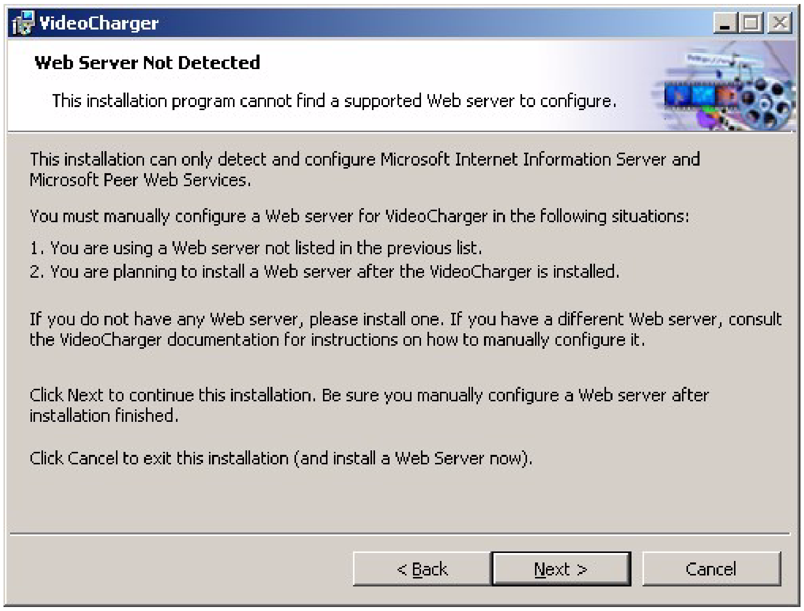
Figure 11-6 *Web Server Detected*

The VideoCharger installation program can detect and automatically configure the following web servers:

- Microsoft Internet Information Server (IIS)
- Microsoft Peer Web Services
- Microsoft Personal Web Server

9. ___ If you have any of these web servers installed on your machine, you will see the window shown in Figure 11-6. In this case, **unselect** the checkbox labelled *Configure VideoCharger Server to work with the selected Web Server* and select **Next** to continue. (Also be sure to disable the Microsoft IIS server by going to the Windows Control Panel and disabling the service named World Wide Web Publishing.)

10. ___ If you do not have any of the above web servers installed on your machine, you will see the window shown in Figure 11-7 on page 344. Because you will be manually configuring the IBM HTTP Server (which was installed during the WebSphere Application Server installation exercise in the Chapter on *Installing Prerequisites*), you select **Next** to continue.



VideoCharger

Web Server Not Detected

This installation program cannot find a supported Web server to configure.

This installation can only detect and configure Microsoft Internet Information Server and Microsoft Peer Web Services.

You must manually configure a Web server for VideoCharger in the following situations:

1. You are using a Web server not listed in the previous list.
2. You are planning to install a Web server after the VideoCharger is installed.

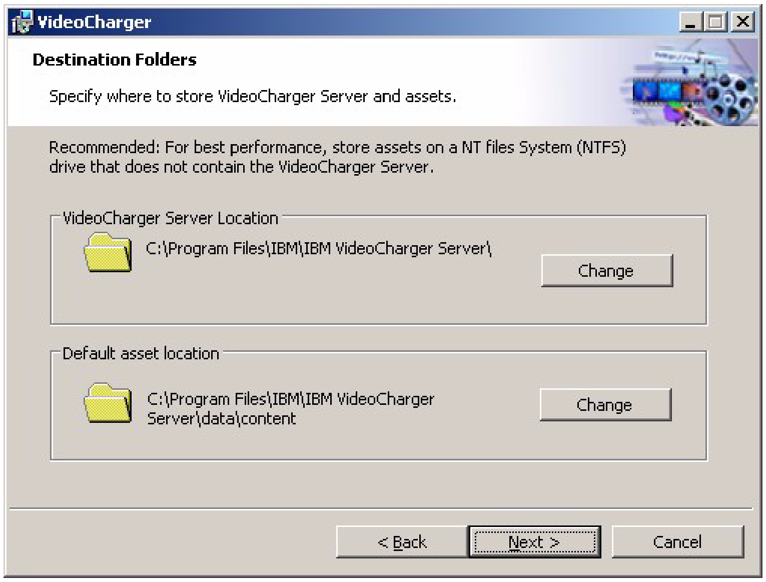
If you do not have any Web server, please install one. If you have a different Web server, consult the VideoCharger documentation for instructions on how to manually configure it.

Click Next to continue this installation. Be sure you manually configure a Web server after installation finished.

Click Cancel to exit this installation (and install a Web Server now).

Figure 11-7 *Web Server Not Detected*

11. ___ Accept the default destination folders and select **Next** to continue, (see Figure 11-8).



Destination Folders

Specify where to store VideoCharger Server and assets.

Recommended: For best performance, store assets on a NT files System (NTFS) drive that does not contain the VideoCharger Server.

VideoCharger Server Location
C:\Program Files\IBM\IBM VideoCharger Server\

Default asset location
C:\Program Files\IBM\IBM VideoCharger Server\data\content

Figure 11-8 *VideoCharger Destination Folders*

12. ___ From the *User Access-Administrator* window, enter **password** as the password for *vsadmin* and select **Next**.

13. ___ From the *Ready to Install the Program* window, select **Install** to begin the file copy process.

14. ___ After the VideoCharger server files have been installed, you may see a window containing post install configuration instructions. Select **Next** to continue. (You will perform these steps in the next section.)

15. ___ Choose to **Automatically start IBM VideoCharger Server services at boot time** and select **Finish** to complete the installation.

VideoCharger Player

The *VideoCharger* player can be used to play media that is streamed from a VideoCharger server. Before starting the VideoCharger player installation, be sure to close all web browser windows (as a browser plug-in will be installed).

1. ___ Start the VideoCharger installation by inserting the VideoCharger CD into the CDROM drive of your workstation.

2. ___ Choose the **English** language for installation and select **OK**.

3. ___ Select **Install Components** from the *Welcome to VideoCharger Installation Launchpad* (see Figure 11-3 on page 340).

4. ___ Choose to **Install VideoCharger Player** and select **Install** (see Figure 11-5 on page 342).

5. ___ From the *Welcome* window, select **Next** to continue.

6. ___ Accept the license agreement and select **Next**.

7. ___ The *Detected Web Browser* window will appear. In order for the web browser plug-in to be installed properly, you must close any open web browser windows at this time. Select **Next** to continue.

8. ___ Choose to perform a **Complete** setup, and select **Next** to continue.

9. ___ Select **Install** to begin the file copy process.

10. ___ Select **Finish** to complete the installation.

Configuration

VideoCharger must be configured before it can be used to stream media to clients. The web server configuration must be updated to allow for a web based VideoCharger administrative interface. The network configuration will be updated to allow the server to use a higher amount of network bandwidth (which improves streaming performance). After configuring the server, you will test the installation by loading a sample media object. The VideoCharger Player will be used to play the media object as it is streamed from the VideoCharger server.

IBM HTTP Server

The VideoCharger installation program can detect and automatically configure the following web servers:

- Microsoft Internet Information Server (IIS)
- Microsoft Peer Web Services
- Microsoft Personal Web Server

Note: You must manually configure any other web server after installing VideoCharger.

During the prerequisite installation exercise, you were instructed to install the IBM HTTP Server (for use with the resource manager). Because the IBM HTTP Server and Microsoft IIS web server both use port 80 by default, you should not have both servers running at the same time. Therefore, be sure the Microsoft IIS service named *World Wide Publishing* is disabled (found in the Windows Services Control Panel). As you will be using the IBM HTTP Server, you must manually configure it for use with VideoCharger.

1. ___ Create an administration and content loading user ID named **vsadmin** by entering the following command from a command prompt:

   "C:\IBM HTTP Server\htpasswd" -c "C:\IBM HTTP Server\conf\vc.passwd" vsadmin

   When prompted for the password, enter ***password***.

2. ___ Open the C:\IBM HTTP Server\conf\httpd.conf file in a text editor like Notepad, and add the following lines to the end of the file:

Note: You can copy and paste these lines from Chapter 11 of the *VideoCharger Installation Guide*.

```
#Start of VideoCharger for NT configuration
DirectoryIndex  default.htm

#Passing environment of VC,these environment variables are very
#important to the CGI programs
PassEnv  LANTV_DIR
PassEnv  LANTV_SDK_DIR

#You must not reverse the order of the following 2 directives.
#ScriptAlias must go before Alias in order to make the CGI work
#Use forward slash for path separator and double quote to quote
#directory with space

#**********************Important ***********************
#Modify the directory value of both ScriptAlias and Alias if you do not
#accept the default VideoCharger for NT installation directory
#****WARNING***
#if any of the following single lines is incorrectly entered
#as two lines in the httpd.conf file the IBM HTTP Server may not start.
ScriptAlias   /lantv/cgi-bin/   "c:/Program Files/IBM/IBM VideoCharger Server/Data/public/cgi-
bin/"
ScriptAlias  /vs_admin/cgi-bin/  "c:/Program Files/IBM/IBM VideoCharger Server/Data/admin/
cgi-bin/"
Alias  /lantv  "c:/Program Files/IBM/IBM VideoCharger Server/Data/public"
Alias  /vs_admin  "c:/Program Files/IBM/IBM VideoCharger Server/Data/admin"
Alias  /content  "c:/Program Files/IBM/IBM VideoCharger Server/data/content"

#Add protection to the CGI-bin directory
#********************Important *********************
#Change the directory reference of if you do not accept the
#default VideoCharger for NT installation directory
<Directory  "c:/Program Files/IBM/IBM VideoCharger Server/Data/admin/html/">
AuthType Basic
AuthUserFile  "c:\IBM HTTP Server\conf\vc.passwd"
#AuthUserFile  "c:\IBM HTTP Server\conf\vc.passwd"
AuthName  "VideoCharger Admin"
require  valid-user
</Directory>

#Disable directory listing
#********************Important *********************
#Change the directory reference of if you do not accept the
#default VideoCharger for NT installation directory
IndexOptions  FancyIndexing

<Directory  "c:/Program Files/IBM/IBM VideoCharger Server/Data/public">
IndexIgnore  *
</Directory>

<Directory  "c:/Program Files/IBM/IBM VideoCharger Server/Data/admin">
IndexIgnore  *
</Directory>

#End of VideoCharger for NT configuration
```

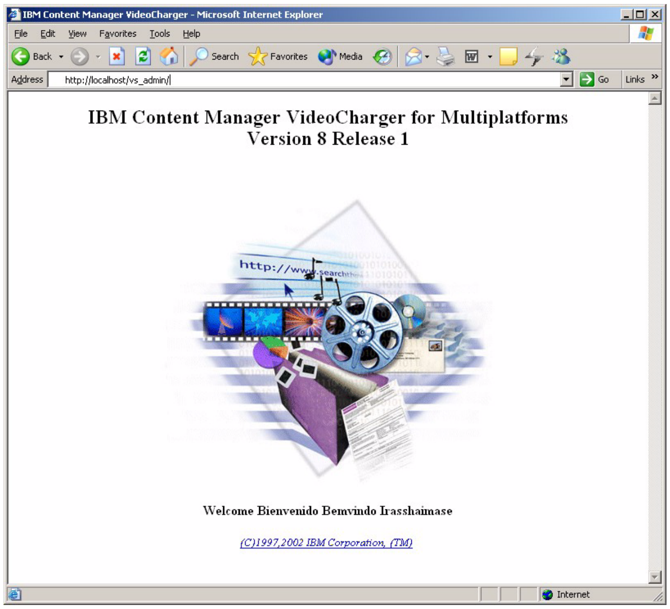
3. ___ **Restart** the IBM HTTP Server.

VideoCharger Server

Once the web server has been configured for VideoCharger, you can use the VideoCharger administrative user ID (*vsadmin*) to review the default configuration.

1. ___ Open a web browser and go to http://localhost/vs_admin/. The

VideoCharger Welcome page should appear, (see Figure 11-9). If you receive an error, review the information entered in the httpd.conf file and restart the web server.


IBM Content Manager VideoCharger - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://localhost/vs_admin/
Go
Links
http://www.search
Internet

IBM Content Manager VideoCharger for Multiplatforms
Version 8 Release 1

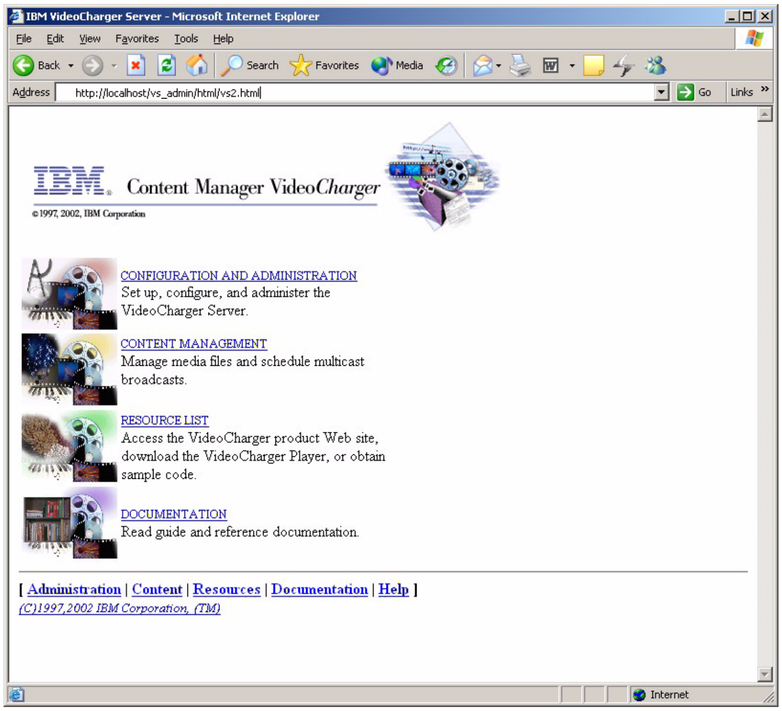
Welcome Bienvenido Bemvindo Irasshaimase

(C)1997,2002 IBM Corporation, (TM)

Figure 11-9 *VideoCharger Administration Welcome Page*

2. ___ Select the **Logo** to log on. When prompted, enter **vsadmin** as the *user ID* and **password** as the *password*. If the logon fails, be sure the *AuthUserFile* parameter entered in the httpd.conf file points to the vc.passwd authentication file you created.

3. ___ From the *Content Manager VideoCharger* page, select **Configuration and Administration**, (see Figure 11-10).


IBM VideoCharger Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/vs_admin/html/vs2.html
Go Links
Internet

IBM. Content Manager VideoCharger

©1997, 2002, IBM Corporation

CONFIGURATION AND ADMINISTRATION
Set up, configure, and administer the VideoCharger Server.

CONTENT MANAGEMENT
Manage media files and schedule multicast broadcasts.

RESOURCE LIST
Access the VideoCharger product Web site, download the VideoCharger Player, or obtain sample code.

DOCUMENTATION
Read guide and reference documentation.

[Administration | Content | Resources | Documentation | Help]
(C)1997,2002 IBM Corporation, (TM)

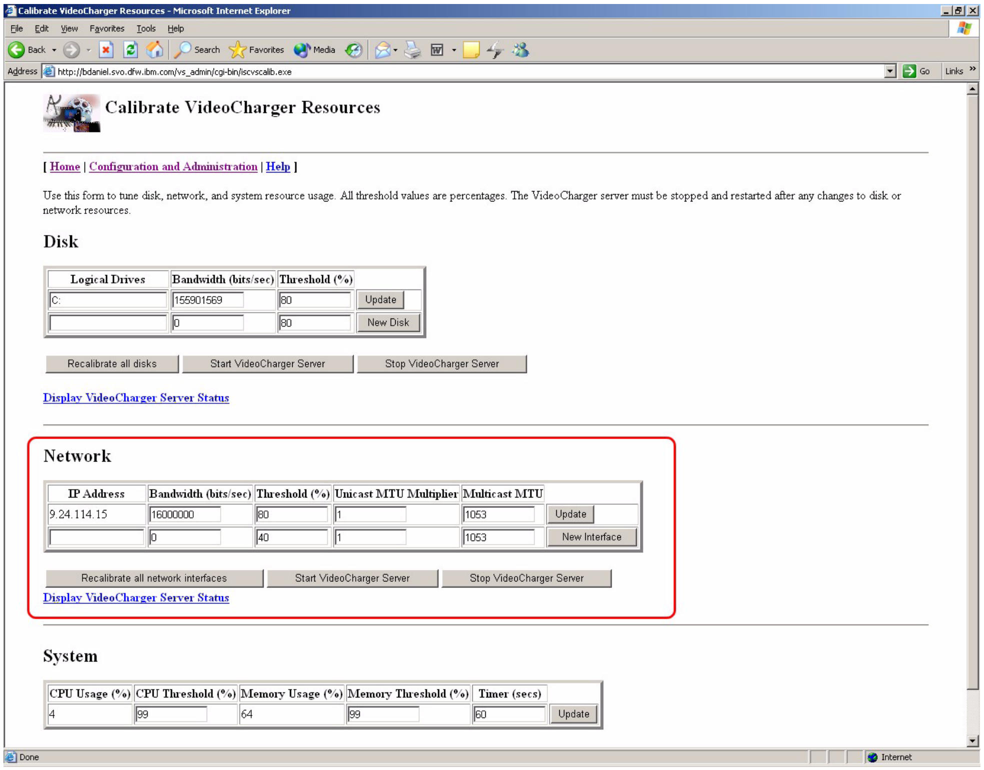
Figure 11-10 *VideoCharger Administration Home panel*

4. ___ From the *Configuration and Administration* page, select **Calibrate VideoCharger Resources**.

5. ___ From the *Calibrate VideoCharger Resources* page, select **Recalibrate all network interfaces**, (see Figure 11-11).

6. ___ Change the *Network Threshold* to 80 and select **Update**. This allows the VideoCharger server to use up to 80% of the network bandwidth in the stream media to clients.

7. ___ Select the **Configuration and Administration** link at the top of the page.



Calibrate VideoCharger Resources - Microsoft Internet Explorer

Address http://bdaniel.svo.dfw.ibm.com/vs_admin/cgi-bin/iscvscalib.exe

Calibrate VideoCharger Resources

[Home | Configuration and Administration | Help]

Use this form to tune disk, network, and system resource usage. All threshold values are percentages. The VideoCharger server must be stopped and restarted after any changes to disk or network resources.

Disk

Logical Drives	Bandwidth (bits/sec)	Threshold (%)	
C:	155901569	80	Update
	0	80	New Disk

Display VideoCharger Server Status

Network

IP Address	Bandwidth (bits/sec)	Threshold (%)	Unicast MTU Multiplier	Multicast MTU	
9.24.114.15	16000000	80	1	1053	Update
	0	40	1	1053	New Interface

Display VideoCharger Server Status

System

CPU Usage (%)	CPU Threshold (%)	Memory Usage (%)	Memory Threshold (%)	Timer (secs)	
4	99	64	99	60	Update

Figure 11-11 *Calibrating Network Devices*

8. ___ From the *Configuration and Administration* page, select **Stop VideoCharger Server**. This stops all VideoCharger services listed in the Windows Services Control Panel. You will see a *completed successfully* message when all VideoCharger services have stopped. (This may take a few minutes, so please be patient.)

9. ___ Select the link labelled **back** button to go back to the *Configuration and Administration* page.

10. ___ From the Configuration and Administration page, select **Start VideoCharger Server**. You will see a *completed successfully* message when all VideoCharger services have started. (This may take a few minutes, so please be patient.)

11. ___ Select the link labelled **back** to go back to the *Configuration and Administration* page.

12. ___ From the *Configuration and Administration* page, select **Display**

VideoCharger Server Status. All services should have an active state.

13. ___ The configuration is now complete, close the web browser window.

Test Configuration

Before integrating VideoCharger with Content Manager, you should validate that media objects can be loaded into the VideoCharger server and streamed to VideoCharger Players. The VideoCharger browser interface can be used to load media assets.

1. ___ Open a web browser and go to http://localhost/vs_admin/. The VideoCharger Welcome page should appear, (see Figure 11-9 on page 349).

2. ___ Select the **Logo** to log on. When prompted, enter **vsadmin** as the user ID and **password** as the password.

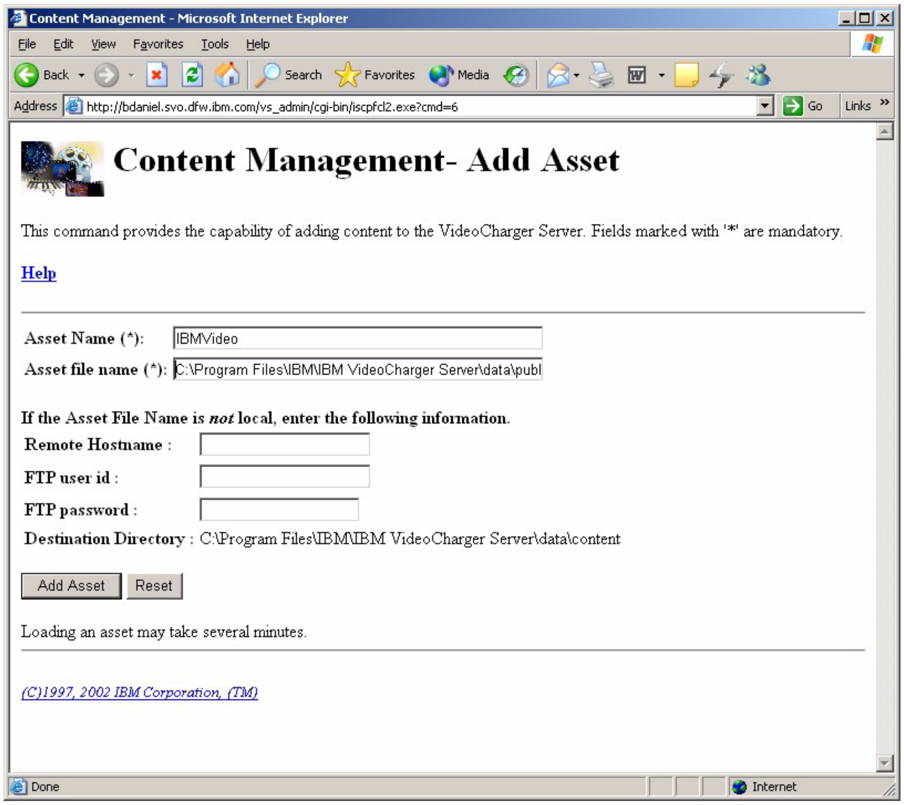
3. ___ From the *Content Manager VideoCharger* page, select **Content Management**, (see Figure 11-10 on page 350).

4. ___ From the *Content Management* page, select **Manage Content**.

5. ___ Choose **Add Local Asset Files** and select **Continue**.

6. ___ From the *Add Local Asset Files* page, select the link labelled **Advanced**.

7. ___ Enter **IBMVideo** as the *asset name*, and **C:\Program Files\IBM\IBM VideoCharger Server\data\public\samples\content\sample15.mpg** as the *asset filename*. Select **Add Asset** to load the video into the VideoCharger server, (see Figure 11-12). You should see an *Operation Completed Successfully* message.


Content Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://bdaniel.svo.dfw.ibm.com/vs_admin/cgi-bin/iscpfcl2.exe?cmd=6
Go Links »
Done
Internet

Content Management- Add Asset

This command provides the capability of adding content to the VideoCharger Server. Fields marked with '*' are mandatory.

Help

Asset Name (*): IBMVideo

Asset file name (*): C:\Program Files\IBM\IBM VideoCharger Server\data\publ

If the Asset File Name is *not* local, enter the following information.

Remote Hostname :

FTP user id :

FTP password :

Destination Directory : C:\Program Files\IBM\IBM VideoCharger Server\data\content

Add Asset Reset

Loading an asset may take several minutes.

(C)1997, 2002 IBM Corporation, (TM)

Figure 11-12 *Adding Video Asset to VideoCharger Server*

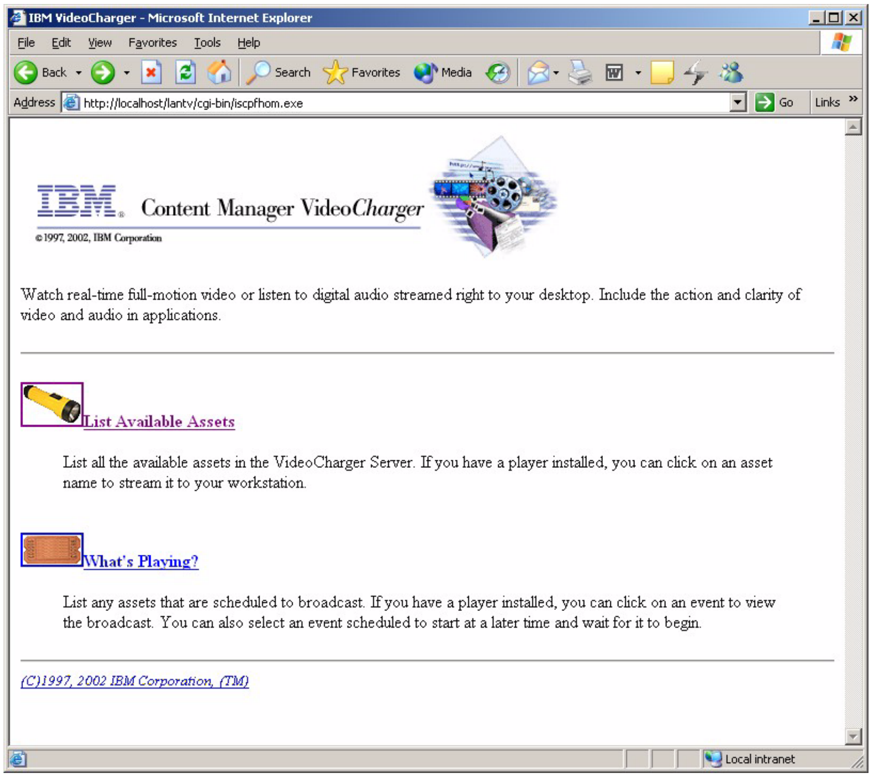
8. ___ **Close** the browser window.

Now that a sample video has been loaded, you can use the VideoCharger Player to test if it will be streamed by the VideoCharger server.

9. ___ Open a web browser and go to http://localhost/lantv/.

10. ___ Select the **Logo** to enter. (By default, a *userid* and *password* is not required for streaming assets through the VideoCharger web interface.)

11. ___ From the Content Manager VideoCharger page, select **List Available Assets**, (see Figure 11-13).


IBM VideoCharger - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/lantv/cgi-bin/iscpfhom.exe
Go Links
IBM Content Manager VideoCharger
©1997, 2002, IBM Corporation
Local intranet

Watch real-time full-motion video or listen to digital audio streamed right to your desktop. Include the action and clarity of video and audio in applications.

List Available Assets

List all the available assets in the VideoCharger Server. If you have a player installed, you can click on an asset name to stream it to your workstation.

What's Playing?

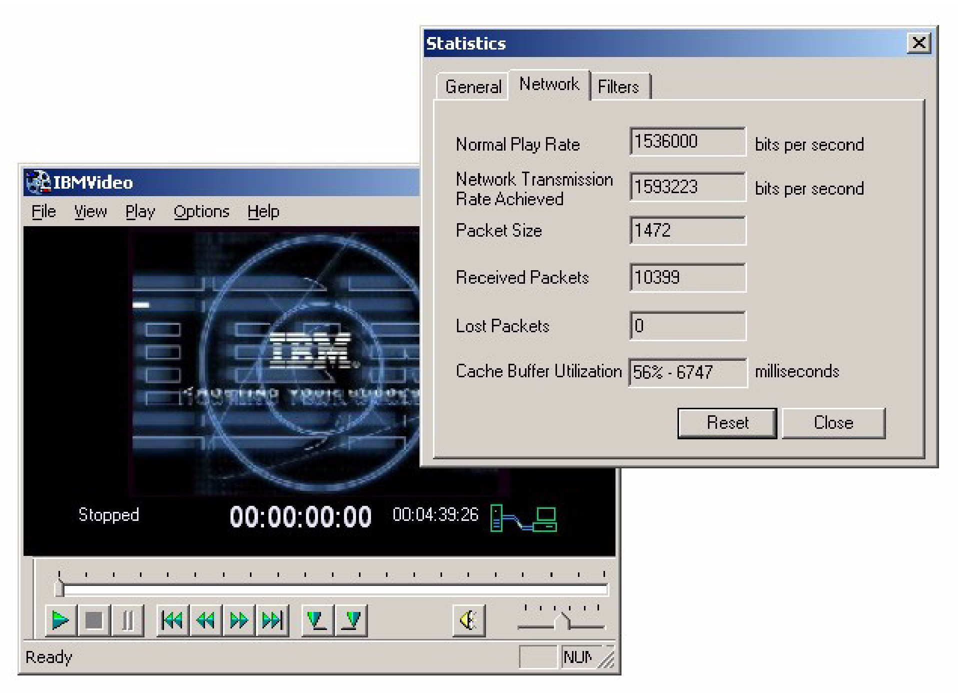
List any assets that are scheduled to broadcast. If you have a player installed, you can click on an event to view the broadcast. You can also select an event scheduled to start at a later time and wait for it to begin.

(C)1997, 2002 IBM Corporation, (TM)

Figure 11-13 *List Available Video Assets*

12. ___ Select **IBMVideo** from the list of available assets. The IBM VideoCharger Player should be automatically launched to play the selected video, (see Figure 11-14).

13. ___ To view statistics on how the video is being streamed over the network, select **Options | Statistics** from the menu bar, (see Figure 11-14).



Normal Play Rate	1536000	bits per second
Network Transmission Rate Achieved	1593223	bits per second
Packet Size	1472	
Received Packets	10399	
Lost Packets	0	
Cache Buffer Utilization	56% - 6747	milliseconds

Stopped 00:00:00:00 00:04:39:26

Ready NUM

Figure 11-14 *Viewing Streaming Video With VideoCharger Player*

14. ___ **Close** the VideoCharger Player and web browser.

Content Manager Integration

Integrating VideoCharger with a resource manager allows you to stream media objects that are managed by Content Manager. In this section, you will learn how to perform this integration. If you have completed the Tivoli Storage Manager integration, the steps in this exercise will be familiar to you. After defining the VideoCharger server to the resource manager and creating a collection for media objects, you will use the Content Manager Windows Client to test the integration.

Define Object Storage

Before Content Manager objects can be stored in a VideoCharger server, the resource manager object storage must be configured. The following steps assume that a VideoCharger server has been installed and configured:

1. ___ Start the *System Administration client* by opening **Start | Programs | IBM Content Manager for Multiplatforms V8.1 | System Administration**.

2. ___ Specify the default *user ID*: **icmadmin** and *password*: **password**. Select **OK** to log on.

3. ___ Expand Resource Manager, then select **RMDB**. At this point, the system administration client will initiate a SSL connection (via https://) between itself and the Resource Manager. Notice the resource manager entities that are available for configuration, (see Figure 11-15).

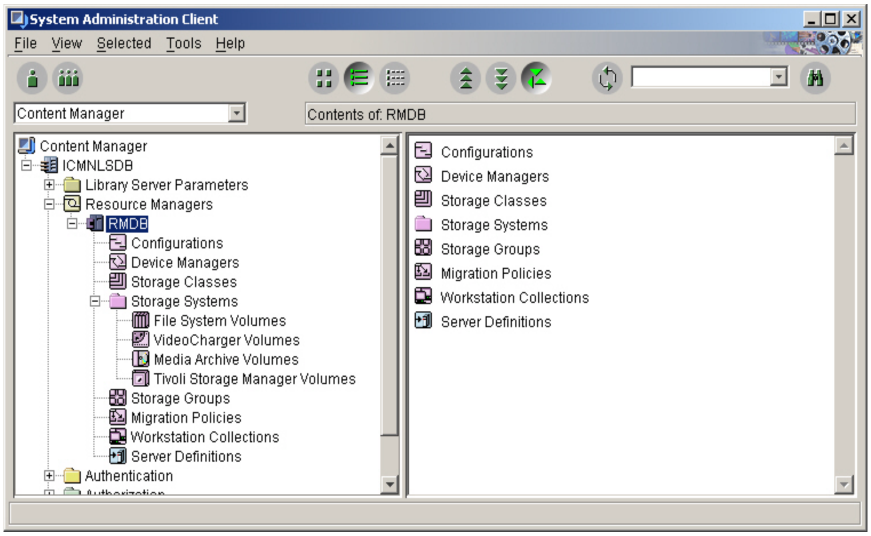
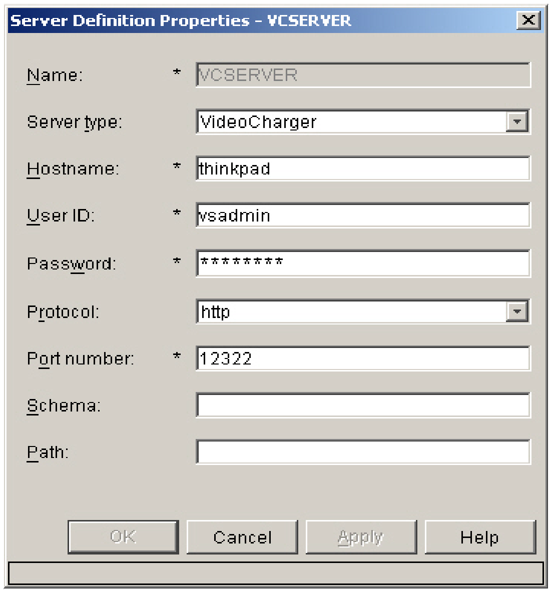


Figure 11-15 *Resource Manager Object Storage Configuration*

4. ___ Define a media manager server by right-clicking on **Server Definitions** and selecting **New**. The *New Server Definition* window will appear, (see Figure 11-16).



Server Definition Properties - VCSERVER

Name: * VCSERVER

Server type: VideoCharger

Hostname: * thinkpad

User ID: * vsadmin

Password: * *********

Protocol: http

Port number: * 12322

Schema:

Path:

Figure 11-16 *New Server Definition*

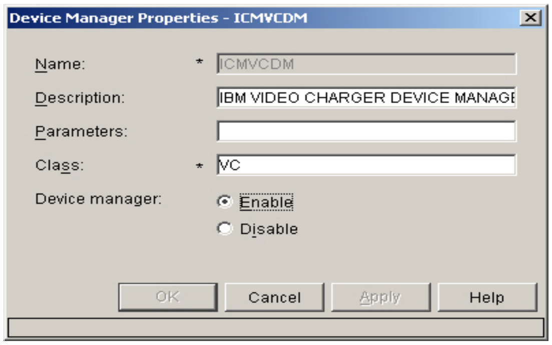
5. ___ Specify the values shown in Table 11-2 and select **OK** to save the VideoCharger server definition.

Table 11-2 *New VideoCharger Server Definition*

Field Name	Field Value
Name	VCSERVER
Server Type	VideoCharger
Hostname	<your machine hostname>
Userid	vsadmin
Password	password
Protocol	http
Port	12322
Schema	
Path	

6. ___ The VideoCharger device manager must be enabled. Right-click on

ICMVCDM (found in the Device Managers folder) and choose **properties**. Choose **Enable** and select **OK** to save, (see Figure 11-17).



Name: * ICMVCDM

Description: IBM VIDEO CHARGER DEVICE MANAGE

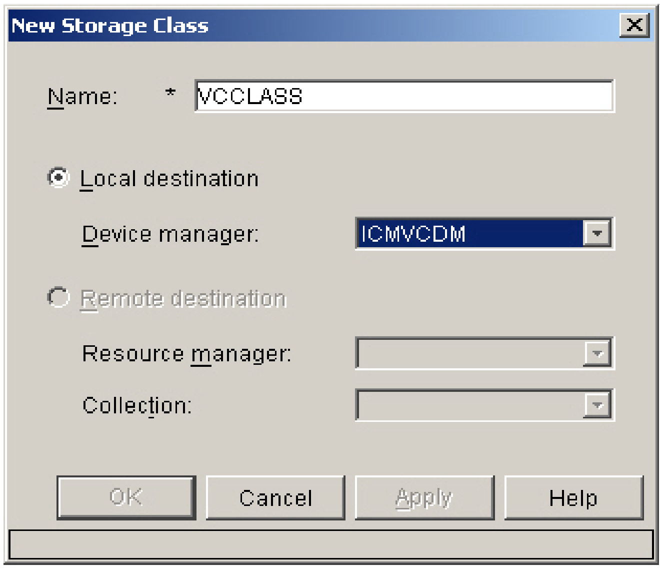
Parameters:

Class: * VC

Device manager: ● Enable ○ Disable

Figure 11-17 *Enabling VideoCharger Device Manager*

7. ___ Define a new storage class by right-clicking on **Storage Classes** and selecting **New**. The *New Storage Class* window will appear, (see Figure 11-18).



Name: * VCCLASS

● Local destination

Device manager: ICMVCDM

○ Remote destination

Resource manager:

Collection:

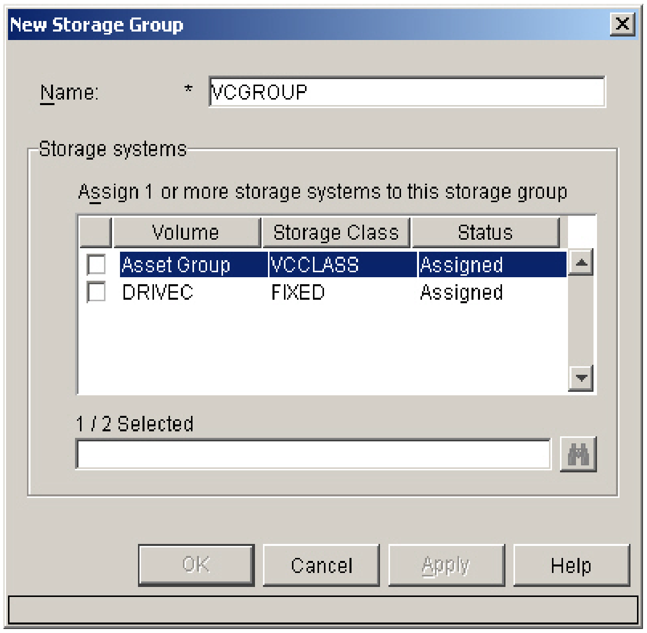
Figure 11-18 *New Storage Class Window*

8. ___ Specify the values shown in Table 11-3 and select **OK** to save the storage class definition.

Table 11-3 *New Storage Class*

Field Name	Field Value
Name	VCCLASS
Device Manager	ICMVCDM

9. ___ Define a new storage group by right-clicking on **Storage Groups** and selecting **New**. The *New Storage Group* window will appear, (see Figure 11-19). Name this storage group **VCGROUP** and select **OK** to save (do NOT select any storage systems at this time).



Name: * VCGROUP

Storage systems

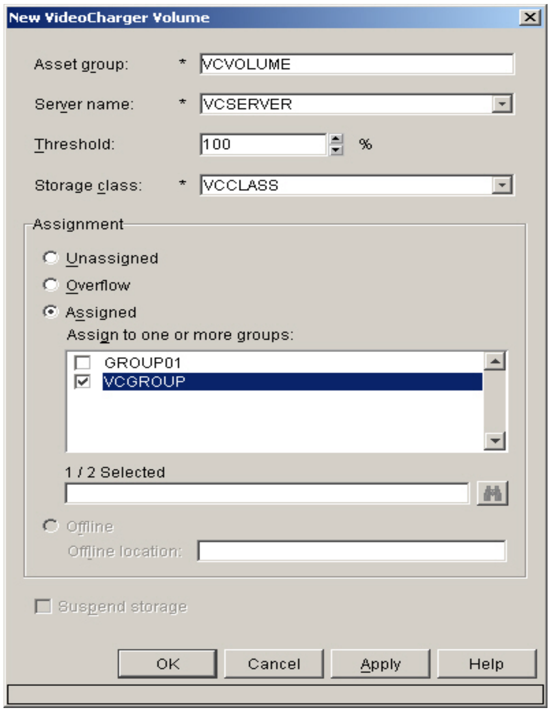
Assign 1 or more storage systems to this storage group

	Volume	Storage Class	Status
□	Asset Group	VCCLASS	Assigned
□	DRIVEC	FIXED	Assigned

1 / 2 Selected

Figure 11-19 *New Storage Group Window*

10. ___ Expand the Storage Systems folder. Define a new VideoCharger volume by right-clicking on **VideoCharger** volumes folder and choose **New**. The *New VideoCharger Volume* window will appear, (see Figure 11-20).



New VideoCharger Volume

Asset group: * VCVOLUME

Server name: * VCSERVER

Threshold: 100 %

Storage class: * VCCLASS

Assignment

○ Unassigned

○ Overflow

● Assigned

Assign to one or more groups:

□ GROUP01

☑ VCGROUP

1 / 2 Selected

○ Offline

Offline location:

□ Suspend storage

Figure 11-20 *New VideoCharger Volume Window*

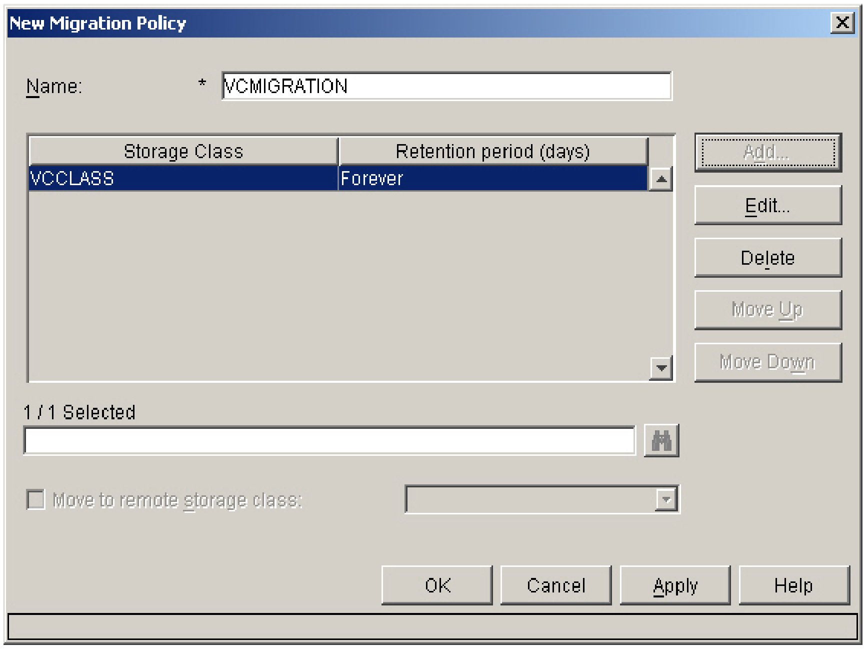
11. ___ Specify the values shown in Table 11-4 and select **OK** to save the volume definition.

Table 11-4 *New VideoCharger Volume*

Field Name	**Field Value**
Name	VCVOLUME
Server Name	VCSERVER
Threshold	100%
Storage Class	VCCLASS
Assignment	Assigned, AND select VCGROUP

12. ___ Define a new migration policy by right-clicking on **Migration Policies**

and selecting **New**. The *New Migration Policy* window will appear, (see Figure 11-21).



Name: * VCMIGRATION

Storage Class	Retention period (days)
VCCLASS	Forever

1 / 1 Selected

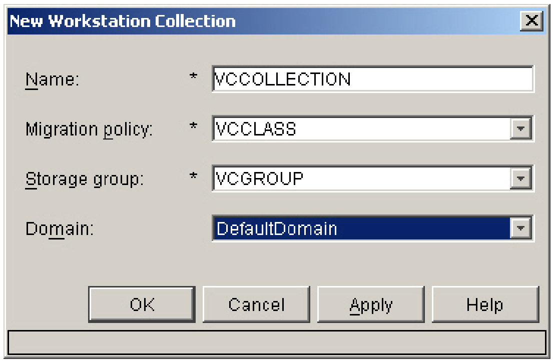
☐ Move to remote storage class:

Figure 11-21 *New Migration Policy Window*

13. ___ Name this migration policy **VCMIGRATION** and select the **Add** button to specify a migration step. Choose **VCCLASS**, and select **forever** as the retention period. Press **OK** to save this migration step.

14. ___ Select **OK** to save the migration policy definition.

15. ___ Define a new collection by right-clicking on **Workstation Collections** and selecting **New**. The New Workstation Collection window will appear, (see Figure 11-22).


New Workstation Collection

Name: * VCCOLLECTION

Migration policy: * VCCLASS

Storage group: * VCGROUP

Domain: DefaultDomain

Figure 11-22 *New Workstation Collection Window*

16. ___ Specify the values shown in Table 11-5 and select **OK** to save the workstation collection definition.

Table 11-5 *New VideoCharger Collection*

Field Name	Field Value
Name	VCOLLECTION
Migration Policy	VCCLASS
Storage Group	VCGROUP
Domain	DefaultDomain

Create Item Type for Videos

In order to test the VideoCharger integration, you must define an item type that uses the collection you created. Once the item type is defined, the Windows Client can be used to load and retrieve media objects.

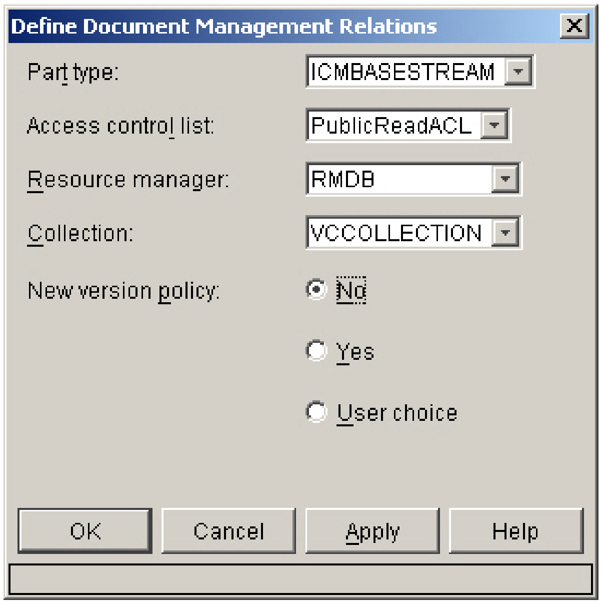
1. ___ Create a new item type by right-clicking on **Item Types** (located under the Data Modeling folder) and selecting **New**.

2. ___ From the Definition tab, type **Video** in the Name field. Leave all other options on this page at their default values.

3. ___ From the tab, add only the attribute named **SOURCE**. Leave the options for this attribute at their default values.

4. ___ From the Document Management window, select the **Add** button. The

Define Document Management Relations window will appear, (see Figure 11-23).



Define Document Management Relations

Part type: ICMBASESTREAM

Access control list: PublicReadACL

Resource manager: RMDB

Collection: VCCOLLECTION

New version policy: ● No ○ Yes ○ User choice

Figure 11-23 *Define Document Management Relations Window*

5. ___Specify the values shown in Table 11-6 Select **OK** to save the item type definition.

Table 11-6 *Define Document Management Relations*

Field Name	Field Value
Part type	ICMBASESTREAM
Access control list	PublicReadACL
Resource manager	RMDB
Collection	VCCOLLECTION
New version policy	No

Import and Play Videos

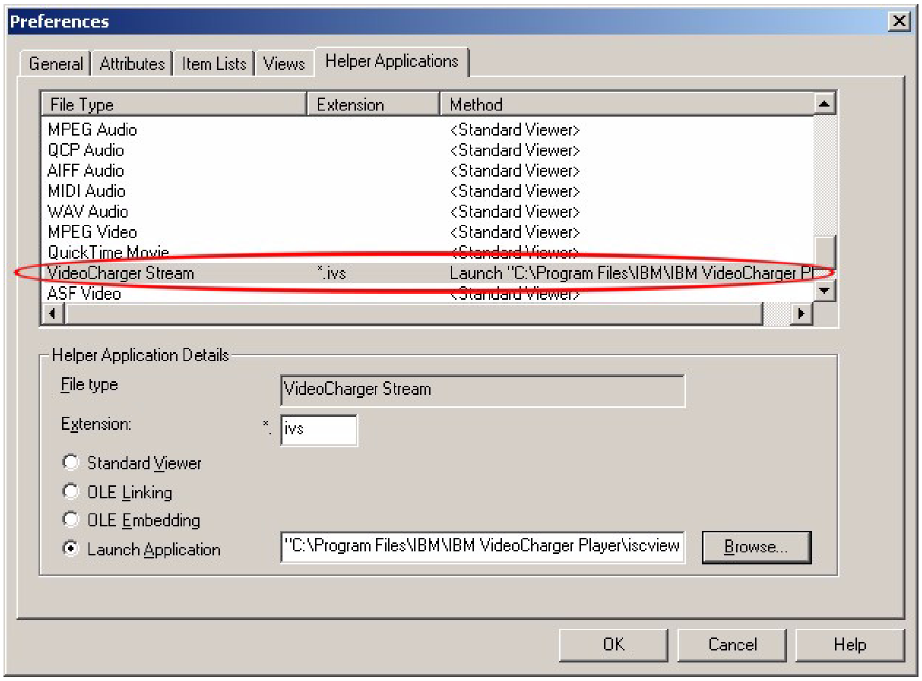
In this section, you will use the Windows Client to import a video into the Video item type. The attributes (metadata) will be stored in the library server while the video file will be stored in the VideoCharger server. You will then use the Windows client to search for and open the video. When opened, the VideoCharger Player will be automatically launched so you can view the video, in real time, as it is being streamed from the VideoCharger Server. (You may also use the Content Manager eClient to test the integration.)

1. ___ Start the Windows Client and log on as **icmadmin**, using **password** as the *password*.

2. ___ The Windows Client must be configured to the launch the VideoCharger Player when a *VideoCharger Stream* document type is opened by the user. Select **Options | Preferences** from the menu bar.

3. ___ Select the tab labelled **Helper Applications**.

4. ___ Find the file type named **VideoCharger Stream**, (see Figure 11-24). Update the extension value to **ivs**. Choose **Launch Application** and specify the value **C:\program files\ibm\IBM VideoCharger Player\iscview.exe**. Select **OK** to save the changes.



File Type	Extension	Method
MPEG Audio		<Standard Viewer>
QCP Audio		<Standard Viewer>
AIFF Audio		<Standard Viewer>
MIDI Audio		<Standard Viewer>
WAV Audio		<Standard Viewer>
MPEG Video		<Standard Viewer>
QuickTime Movie		<Standard Viewer>
VideoCharger Stream	*.ivs	Launch "C:\Program Files\IBM\IBM VideoCharger Pl
ASF Video		<Standard Viewer>

Helper Application Details

File type: VideoCharger Stream

Extension: *. ivs

○ Standard Viewer

○ OLE Linking

○ OLE Embedding

● Launch Application "C:\Program Files\IBM\IBM VideoCharger Player\iscview

Figure 11-24 *Adding VideoCharger Stream Helper Application*

5. ___ Select **File | Import** from the menu bar.

6. ___ Specify the values shown in Table 11-7. Be sure to select the correct file type, (see Figure 11-25). Select **Import** to load the video file.

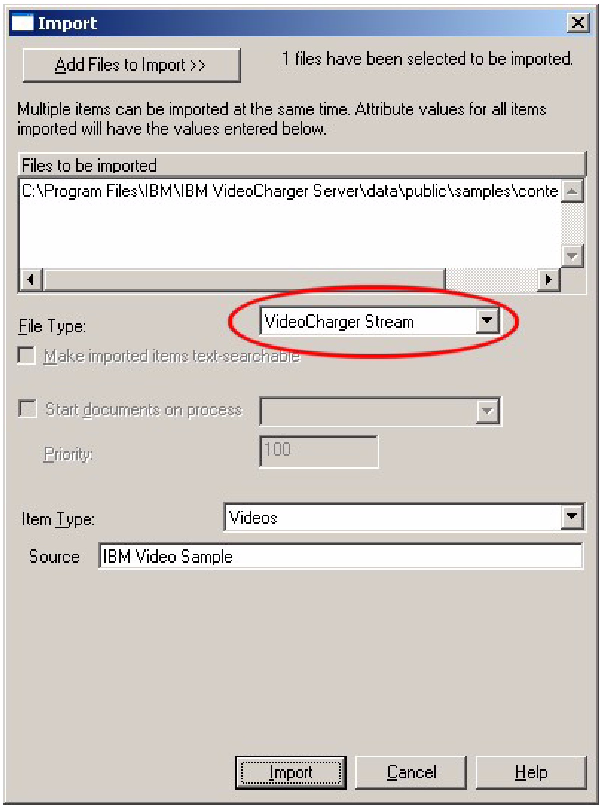
Note: The *sample15.mpg* sample video is approximately 50MB in size and will take a few minutes to import.

Table 11-7 *Importing Video File*

Field Name	Field Value
Files to be imported	C:\Program Files\IBM\IBM VideoCharger Server\data\public\samples\content\sample15.mpg
File Type	VideoCharger Stream
Item Type	Videos

Table 11-7 *Importing Video File*

Field Name	Field Value
Source (attribute)	IBM Sample Video



1 files have been selected to be imported.

Multiple items can be imported at the same time. Attribute values for all items imported will have the values entered below.

Files to be imported

C:\Program Files\IBM\IBM VideoCharger Server\data\public\samples\conte

File Type: VideoCharger Stream

□ Make imported items text-searchable

□ Start documents on process

Priority: 100

Item Type: Videos

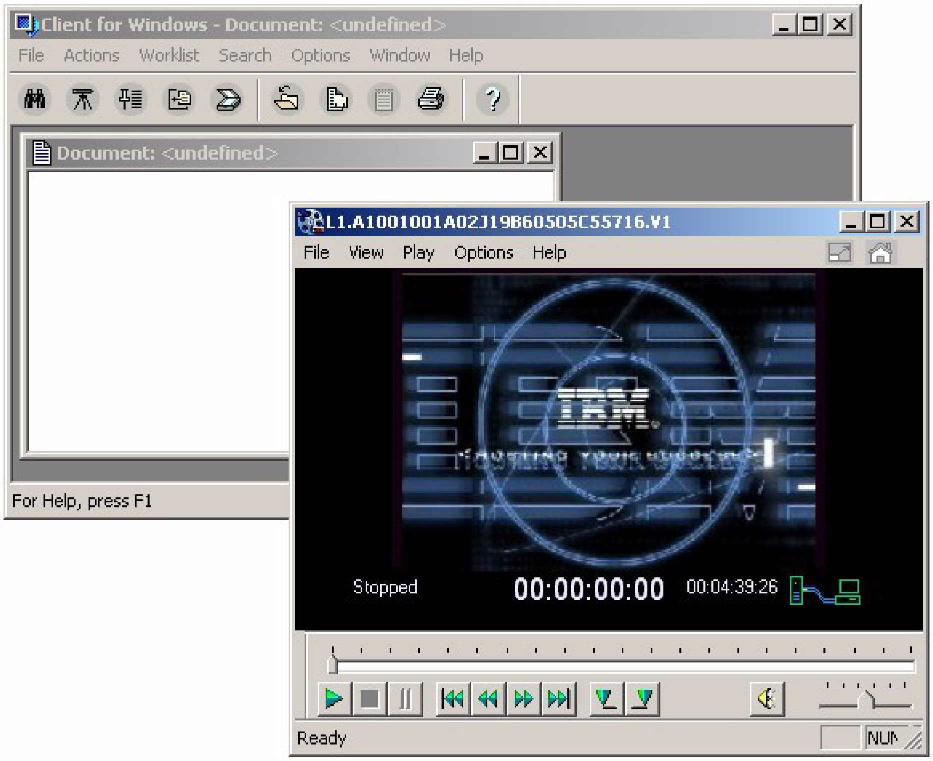
Source IBM Video Sample

Figure 11-25 *Importing Video From Windows Client*

Note: If using the eClient to import a video, the file type should be `video/x-ibm-ivs` and the content type should be *multimedia streaming document*.

7. ___ Perform a basic search for this video in the item type **Video**.

8. ___ Choose to open the video. The VideoCharger Player will be launched, and the video file will begin to be *streamed* from the VideoCharger server to the player, (see Figure 11-26).



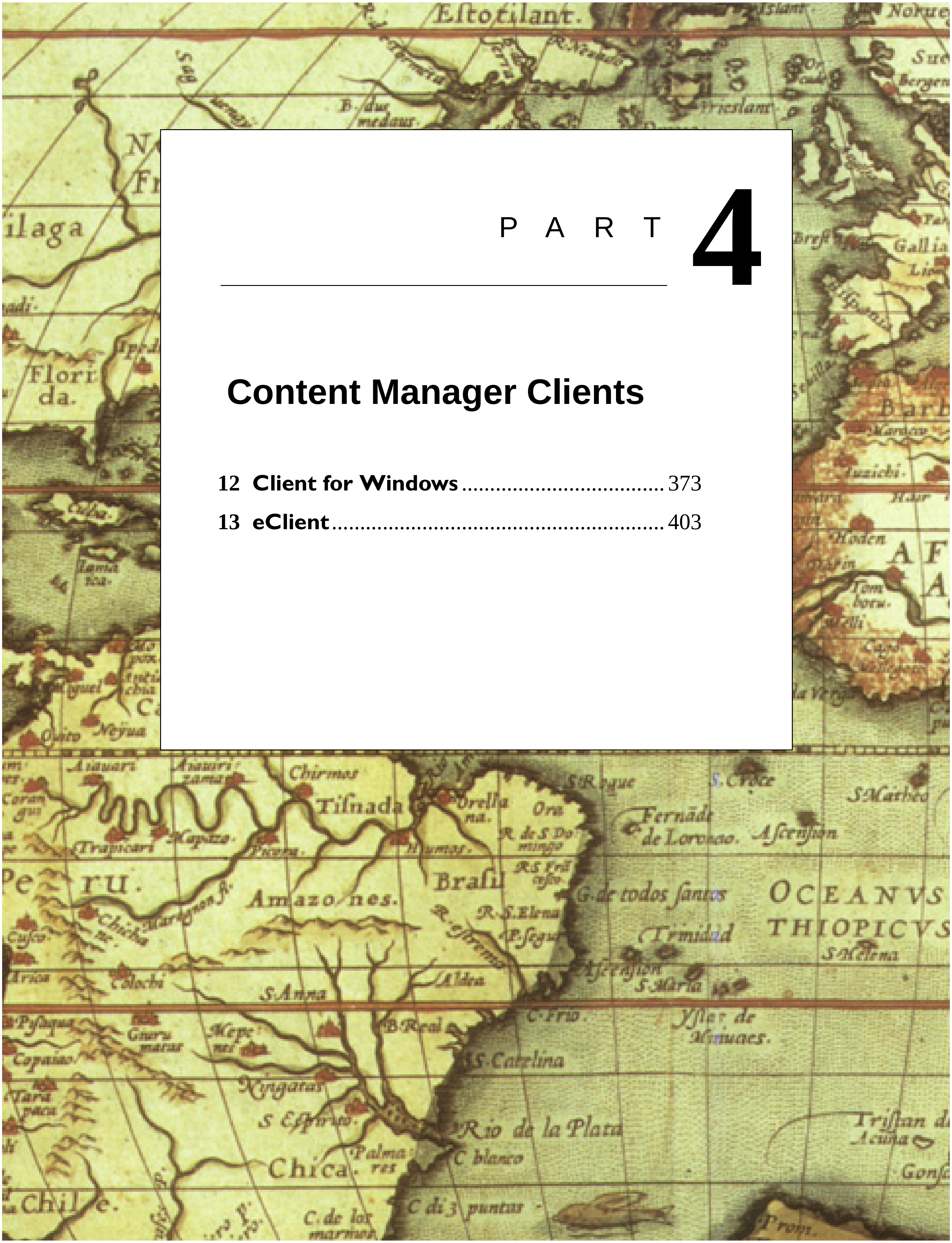
Client for Windows - Document: <undefined>
File Actions Worklist Search Options Window Help
Document: <undefined>
For Help, press F1
L1.A1001001A02J19B60505C55716.V1
File View Play Options Help
Stopped
00:00:00:00
00:04:39:26
Ready
NUM

Figure 11-26 *Viewing a Video From Windows Client*

Summary

In this chapter, you were introduced to IBM VideoCharger and how it can be used with IBM Content Manager for Multiplatforms. You learned that VideoCharger can stream media objects to clients and can also manage the storage of media files (which are usually quite large). By streaming media files, clients can view them as it is being downloaded. Without the streaming capability, a client will have to wait for the entire media file to be downloaded to the workstation before being able to view it.

Integrating Content Manager with VideoCharger allows you to provide complex search and access control capabilities while leveraging the streaming and storage management functionality of VideoCharger. The Content Manager library server will contain the metadata (attribute and item type values) and access control policies for your media objects. You learned that the VideoCharger integration involves the configuration of the resource manager object storage and the definition of an item type that uses the ICMBASESTREAM part. When a user makes a requests for one of these media objects, it will be streamed from the VideoCharger server to the client workstation.



PART 4

Content Manager Clients

CHAPTER 12

Client for Windows

- Importing Using Item Types
- Searching for Items
- Using Text Search
- Using Document Routing

In this chapter, the Content Manager Client for Windows will be used to demonstrate the use of the new data model. Along with importing items into Content Manager, this section will point out how items are identified for text search indexing and how items are added to a document routing process. Once the items have been imported the different client options will be used to perform text searches and alter items on the document routing process. The *IBM Certification Solutions Expert (CSE) - IBM Content Manager Version 8 Certification Exam 442* does contain questions concerning how the Client for Windows uses item types, text search, and document routing options.

Importing Using an Item Type

The steps in this section will cover importing images into the PhotoLab item type created in Chapter 6 *Defining the Data Model*.

1. ___ Start the **Client for Windows**.

   Start | Programs | IBM Content Manager V8 | Client for Windows.

2. ___ Specify the default *user ID* **icmadmin** and **password**.

   The Library Server name should show **icmnlsdb** if the default install options have been taken.

3. ___ Press **OK** to logon.

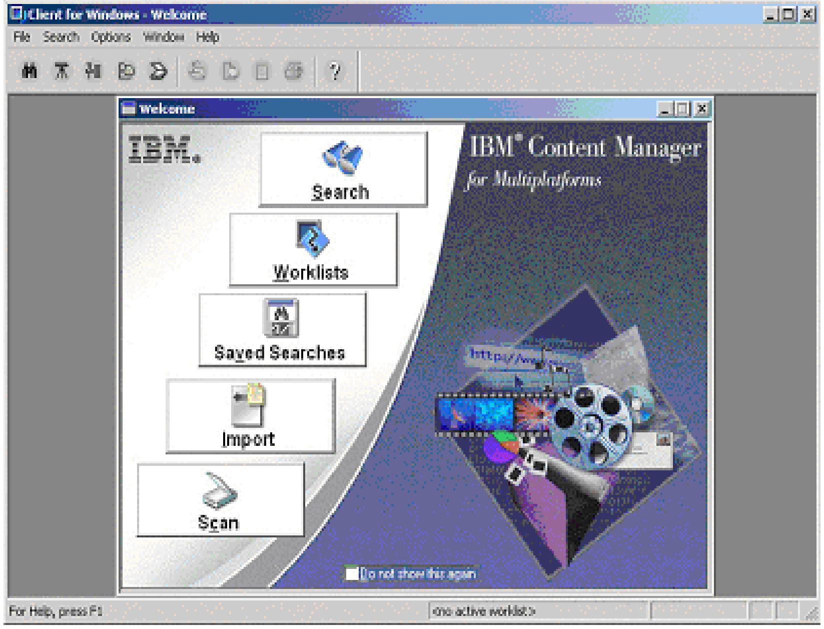


Figure 12–1 *Windows Client Welcome Screen*

4. ___ Select the **Import icon** on the Client for Windows Welcome screen, (see Figure 12–1).

   A similar procedure is used if you were scanning objects directly into Content Manager.

5. ___ On the **Import** screen, select **Add Files to import**.

6. ___ On the **Open** dialog choose **x:\Photos**.

   The PhotoLab scenario assumes that JPEG photos are stored in a directory on the computer's main drive. At this point, select any image file you might have to import into the system. If you do not have an image or photo, use a document file or text file that can be viewed in the Client for Windows.

7. ___ Highlight a number of photos using the keyboard SHIFT Key and/or Mouse Select Button.

   You can also use the CTRL and Mouse Select Button to independently choose photos.

8. ___ Select **Open** to return to the Import screen.

9. ___ Select **JPEG Image** as the *File Type*.

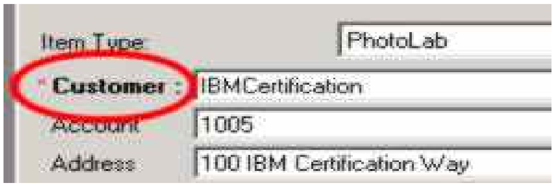
10. ___ Select **PhotoLab** as the item type.

11. ___ The root level attributes defined for this item type are displayed. Use Table 12–1 to type values for the displayed attributes.

Table 12–1 *PhotoLab attribute values*

Attribute	Value
Account	1005
*Customer	Use your name.
Address	Enter the address of your office
Phone	XXX-IBM-CERT
Category	For now leave blank.

12. ___ Notice the **Customer** attribute is bold and has an * in Figure 12–2 on page 376. This is because in the item type the attribute was marked as required and represents the item.



Item Type: PhotoLab

* Customer : IBMCertification

Account: 1005

Address: 100 IBM Certification Way

Figure 12–2 *Item type required attribute.*

13. ___ Notice the **Order** attribute representing the child component or child level of attributes, (see Figure 12–3).

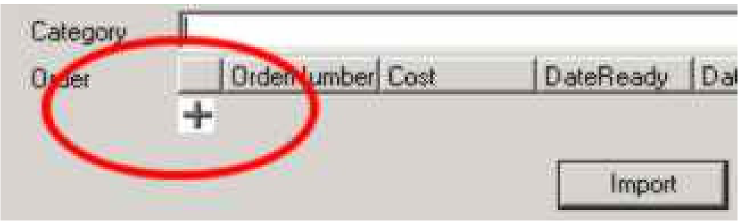


Figure 12–3 *Add child level component attributes*

14. ___ Select (+) plus sign next to the *Order* child attribute level name, (see Figure 12–3).

15. ___ Use the table Table 12–2 to complete the child level attributes by selecting the (+) plus sign for each row of data to be added.

Table 12–2 *Child level attribute information*

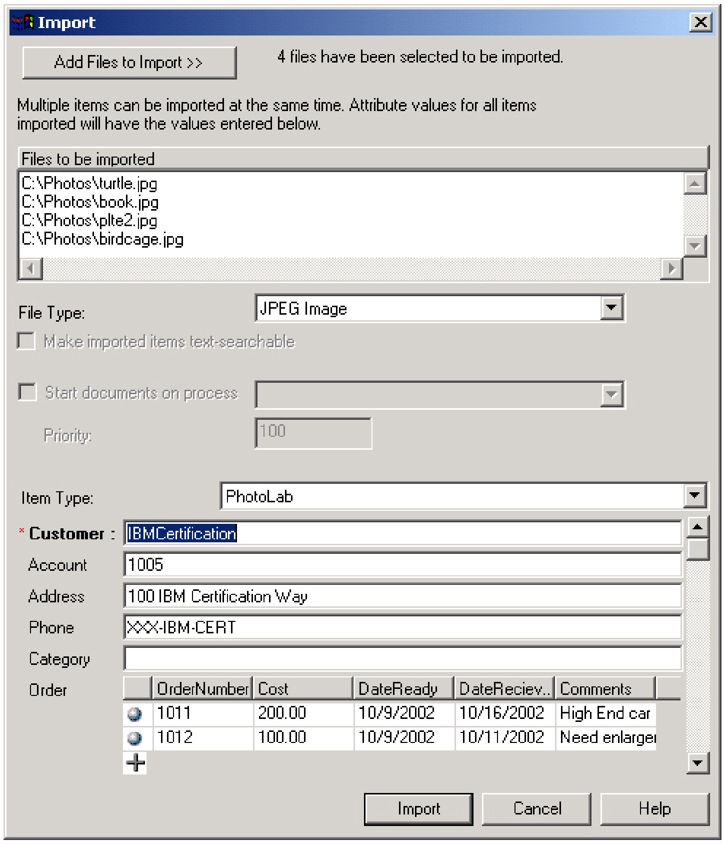
Order Number	Costs	DateReceived	Dateready	Comments
1011	200.00	Select today's date.	Select date for the end of the week.	High End car photos to touch up.
1012	100.00	Select today's date.	Select date for the end of the week.	Need enlargements.

16. ___ The import screen should resemble Figure 12–4 on page 377.

17. ___ Notice that all the images or photos imported will be assigned the same attributes typed on the screen.

18. ___ Select **Import**.

19. ___ A busy bar will be shown while the photos are imported. When done you can import additional photos.



Import

4 files have been selected to be imported.

Multiple items can be imported at the same time. Attribute values for all items imported will have the values entered below.

Files to be imported

C:\Photos\turtle.jpg
C:\Photos\book.jpg
C:\Photos\plte2.jpg
C:\Photos\birdcage.jpg

File Type: JPEG Image

☐ Make imported items text-searchable

☐ Start documents on process

Priority: 100

Item Type: PhotoLab

* **Customer :**	IBMCertification
Account	1005
Address	100 IBM Certification Way
Phone	XXX-IBM-CERT
Category	

Order

	OrderNumber	Cost	DateReady	DateReciev..	Comments
●	1011	200.00	10/9/2002	10/16/2002	High End car
●	1012	100.00	10/9/2002	10/11/2002	Need enlarger
+					

Figure 12–4 *Windows Client Import Screen*

20. ___ Select **Cancel** to close the *Import* screen.

Note: With the above item type text documents or documents for which Content Manager has file converters can be imported and made text searchable by selecting **Make imported items text searchable** on the Client for Windows import screen , (see Figure 12–4 on page 377).

Searching for Imported Images

With photos imported into the system, use the Content Manager Client for Windows basic search to search for photos. This section will show how the client presents the child level attributes for query.

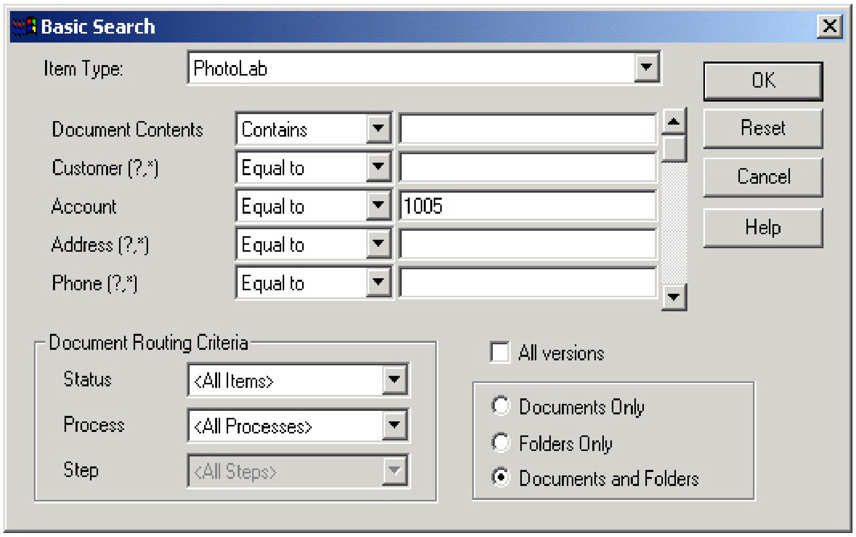
1. ___ Select **Search.**

   If from the menu bar then also select **Basic.** If from the Content Manager Client for Windows startup screen, the search icon displays **Basic Search**.

2. ___ Select **PhotoLab** as the item type.

   This is the item type used to import images.

3. ___ Type **1005** as the value for the **Account**.



Basic Search

Item Type: PhotoLab

Document Contents: Contains

Customer (?,*): Equal to

Account: Equal to 1005

Address (?,*): Equal to

Phone (?,*): Equal to

Document Routing Criteria

Status: <All Items>

Process: <All Processes>

Step: <All Steps>

□ All versions

○ Documents Only
○ Folders Only
● Documents and Folders

Figure 12–5 *Client for Windows basic search*

4. ___ In Figure 12–5 notice by moving the scroll bar that the Basic Search panels list all the attributes for the item type including the child levels in sequential order.

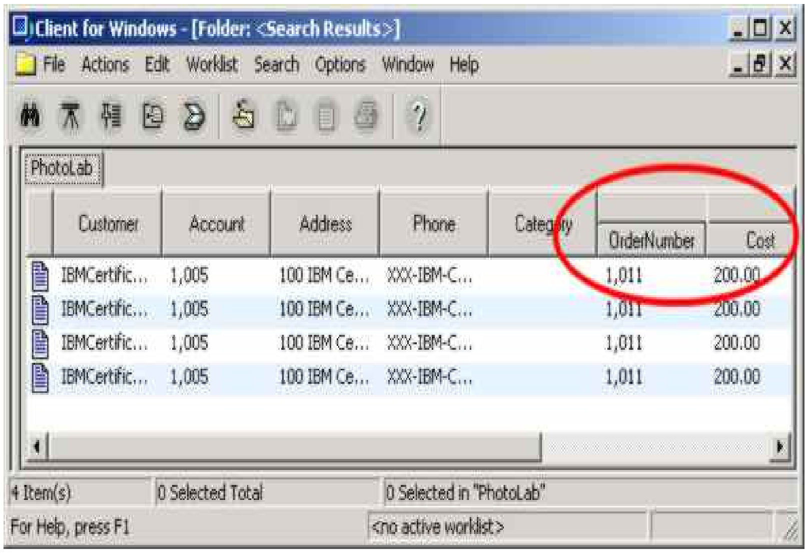
5. ___ In Figure 12–5 notice the *Document Contents* search line. This is not for an attribute search, but present because the item type and parts added were enabled for text search. Strings entered on this line perform a content search against the indexed data.

Note: When the PhotoLab item type was setup, text search was selected on the item type Definition screen, on the Document Management part assignment screen, and could also have been selected for each of the attributes. Strings entered on the *Document Content* line searches the contents of the loaded documents, using *contains* on the attribute lines performs an index search on the attributes.

6. ___ In Figure 12–5 on page 378 notice the check box for **All versions.** If selected then the attributes for all versions of an item will be displayed.

7. ___ In Figure 12–5 on page 378 notice the options to search for Documents, Folders (document classification with no parts), or both.

8. ___ Select **OK**.



Customer	Account	Address	Phone	Category	OrderNumber	Cost
IBMCertific...	1,005	100 IBM Ce...	XXX-IBM-C...		1,011	200.00
IBMCertific...	1,005	100 IBM Ce...	XXX-IBM-C...		1,011	200.00
IBMCertific...	1,005	100 IBM Ce...	XXX-IBM-C...		1,011	200.00
IBMCertific...	1,005	100 IBM Ce...	XXX-IBM-C...		1,011	200.00

4 Item(s)

0 Selected Total

0 Selected in "PhotoLab"

For Help, press F1

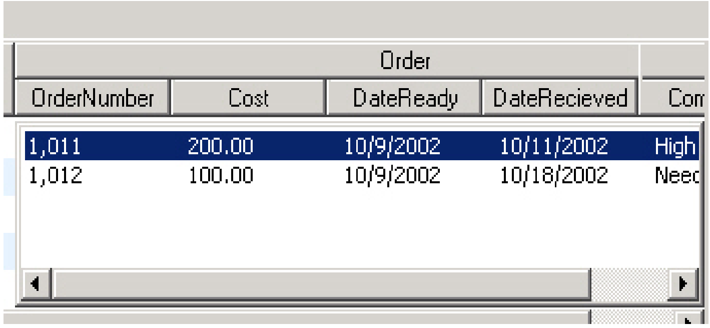
<no active worklist>

Figure 12–6 *Client for Windows search results*

9. ___ On the search results screen Figure 12–6, notice how the child level attributes were initially listed. When the images were saved, two values were entered for each of the attributes listed under the child component **Order**.

10. ___ Select one of the **attribute values** under the *child component Order.*

11. ___ An attribute window, (see Figure 12–7) is displayed listing the values entered for each row of the child level component.



Order				
OrderNumber	Cost	DateReady	DateRecieved	Com
1,011	200.00	10/9/2002	10/11/2002	High
1,012	100.00	10/9/2002	10/18/2002	Neec

Figure 12–7 *Client for Windows child level or multi-value attributes*

12. ___ Select and open one of the listed images.

Note: Content Manager multi-value attributes are supported using a child level component or child level attributes. It is important to realize that the Client for Windows only supports the first child level. Attributes added to an item type child level beyond the first will not be visible in the Client for Windows.

Search Using Item Type for Folders

Now do a search using the item type setup to function as a folder. Because the PhotoLab item type and MyPhotoWork item are linked together, MyPhotoWork can be used to locate items. If auto-foldering is working correctly searching MyPhotoWork using the same attributes as done in the steps above should display the same list of items.

1. ___ Select **Search.**

2. ___ Select **Basic**.

3. ___ Select **MyPhotoWork** as the item type.

4. ___ Type **1005** as the value for **Account**.

5. ___ Select **OK**.

A screen similar to Figure 12–6 should be displayed.

Using Text Search

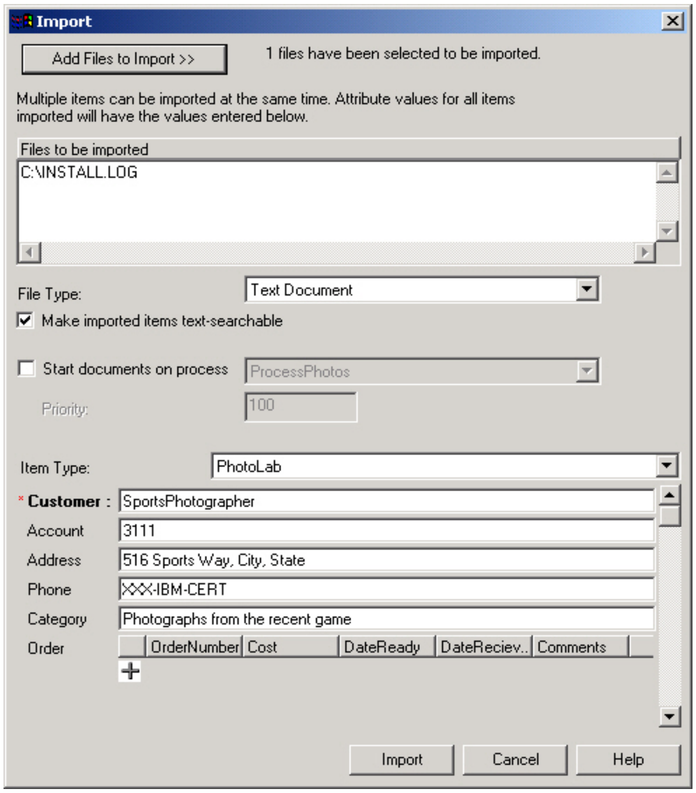
Documents, text files, and other document objects for which Content Manager provides conversions can be imported and identified for text indexing. Once the files are imported, they are processed by the DB2 UDB Text Information Extender to create the indexed values. The values are stored on the server in the directory indicated when the item type was created.

1. ___ Select **Import**.
2. ___ Select **Add Files to Import**.
3. ___ On the *Open* dialogue choose some text files.
4. ___ Select **Open** to return to the Import Object screen.
5. ___ Select **Text Document** as the *File Type*.
6. ___ Select **Make imported items text-searchable**
7. ___ Select **PhotoLab** as the item type.
8. ___ Use Table 12–3 to complete the import attributes.

Table 12–3 *Attributes values used for text search*

Attribute	Value
*Customer	SportsPhotographer
Account	3111
Address	516 Sports Way, City, State
Phone	XXX-IBM-CERT
Category	GamePhotos

9. ___ For now, ignore the attributes for the *Order* child levels. The screen should resemble Figure 12–8.



1 files have been selected to be imported.

Multiple items can be imported at the same time. Attribute values for all items imported will have the values entered below.

Files to be imported
C:\INSTALL.LOG

File Type: Text Document

☑ Make imported items text-searchable

☐ Start documents on process ProcessPhotos

Priority: 100

Item Type: PhotoLab

* **Customer :**	SportsPhotographer
Account	3111
Address	516 Sports Way, City, State
Phone	XXX-IBM-CERT
Category	Photographs from the recent game
Order	OrderNumber | Cost | DateReady | DateReciev.. | Comments

Figure 12–8 *Import screen for importing items to be indexed*

10. ___ Select **Import**.

11. ___ Select Cancel to close the **Import** screen.

Now do a basic search to locate the documents. You may need to give it a few minutes to allow the text search indexing process to complete.

12. ___ Open the **Basic Search** screen.

13. ___ Select **PhotoLab**.

14. ___ Type a text string that was contained in the imported documents into the **Document Contents** field.

15. ___ Select **OK**.

Documents that contain text matching the entered string will be listed in the search results list. If only one document exists, then it will be displayed.

Using Document Routing

The Content Manager Client for Windows provides support for starting documents, images, and other files on a document routing process when scanned or imported. In addition, previously imported objects and folders the user has access to can be started on a document routing process. Once objects and folders are started on a document routing process, the Client for Windows user uses the worklists they can access to work with items residing on the different work nodes. The *process* action menu provides the actions the user can take on objects and folders represented in the worklist contained work package. The available actions are based on how the work node, where the object or folder resides, was defined. What process actions where defined for moving items onto the next step in the process. Along with the ability to take action on process objects or folders, the Client for Windows search facility provides support for searching items in a process based on its status, process, or step in the process.

This section assumes that the document routing processes, work nodes and worklists identified in the *Building Document Routing* section of this guide have been defined. The following steps will point out some of the Client for Windows support for document routing using the defined model in the Chapter on *Building Document Routing.*

1. ___ Start the **Client for Windows**.

   Start | Programs | IBM Content Manager V8 | Client for Windows.

2. ___ Specify the default *user ID* **icmadmin** and **password**.

   The Library Server name should show **icmnlsdb** if the default install options have been taken.

3. ___ Press **OK** to logon.

4. ___ Select **Worklists** on the Client for Windows welcome screen.

5. ___ The Worklist window should open displaying three worklists: PhotoOrders, ProblemPhotoJobs, and ProcessedPhotos.

   Each worklist should show 0 items in the worklist. The item count may not be displayed as it is a user preference. For the following exercises it would be beneficial to have the item count on.

6. ___ Select the Client for Windows **Options** menu.

7. ___ Select **Preferences** on the Options menu.

8. ___ Select **Item Lists** on the preferences screen.

Note: The item count does not update automatically as items are added and removed from the worklist. Use the ***Refresh Item Count*** on the Windows menu to refresh the item counts.

9. ___ Make sure the **Display number of items in worklist** has been selected.
10. ___ It would also be beneficial to select both **Display alternating rows with a different background color** and **Display Child Components with a different background color**. This will make the list of items easier to view.
11. ___ Also set the **Rows of multiple values to display** to **2**.
12. ___ Select **OK**.

Assigning Items to a Process

This section will use the ProcessPhotos document routing process to demonstrate the options on import that apply to document routing.

Note: Documents, images, and other files imported and started directly on a document routing process from the import screen flow directly through a defined document routing collection work node. The collection work node only holds items when a folder defined in the collection resume list has been started on the document routing process.

1. ___ Select **File** | **Import**.
2. ___ On the Import screen, select **three files to import**.
3. ___ Select the correct **File Type** for the items being imported.
4. ___ Select **Start documents on process.**
5. ___ Select **ProcessPhotos** as the process.
6. ___ Do not alter the priority.
7. ___ Select **PhotoLab** for the item type.

8. ___ Use Table 12–4 to enter the attribute values for the imported items.

Table 12–4 *Attribute values for imported process items*

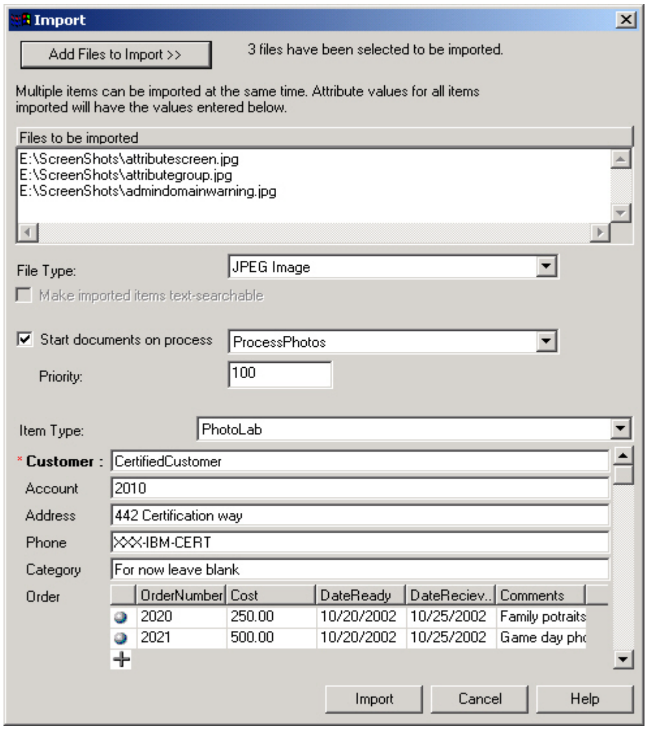
Attribute	Value
Account	2010
*Customer	CertifiedCustomer
Address	442 Certification way
Phone	XXX-IBM-CERT
Category	For now leave blank.

9. ___ Use Table 12–5 to complete the attribute values for the child level component Orders.

Table 12–5 *Attribute values for the process item child orders*

Order Number	Costs	DateReceived	Dateready	Comments
2020	250.00	Select today's date.	Select date for the end of the week.	Family portraits.
2021	500.00	Select today's date.	Select date for the end of next week.	Game day photographs.

10. ___ The import screen should resemble Figure 12–9.



3 files have been selected to be imported.

Multiple items can be imported at the same time. Attribute values for all items imported will have the values entered below.

Files to be imported
E:\ScreenShots\attributescreen.jpg
E:\ScreenShots\attributegroup.jpg
E:\ScreenShots\admindomainwarning.jpg

File Type: JPEG Image

☐ Make imported items text-searchable

☑ Start documents on process ProcessPhotos

Priority: 100

Item Type: PhotoLab

* **Customer :**	CertifiedCustomer
Account	2010
Address	442 Certification way
Phone	XXX-IBM-CERT
Category	For now leave blank

Order

OrderNumber	Cost	DateReady	DateReciev..	Comments
2020	250.00	10/20/2002	10/25/2002	Family potraits
2021	500.00	10/20/2002	10/25/2002	Game day pho

Figure 12–9 *Import screen with document process selected.*

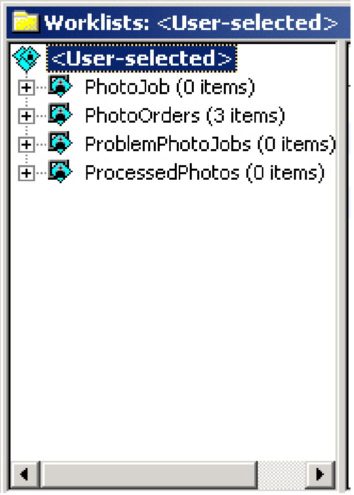
11. ___ Select **Import**.

12. ___ After importing **close** the **Import screen.**

13. ___ **Open** the **Worklists** (File | Worklists).

14. ___ Notice in Figure 12–10 on page 387 that the PhotoJob worklist contains 0 items.

PhotoJob is the worklist that represents the first work node of the process. One would expect that the items would remain on the first process until the resume requirements are met or the user takes an action. The reason the items have proceeded directly on to the second node represented by PhotoOrders is that documents (or files) assigned directly to a document routing process do not apply to the collection work node constraints. Also, folders assigned to a process where the resume list does not contain the folder item type will also proceed directly through the collection work node.



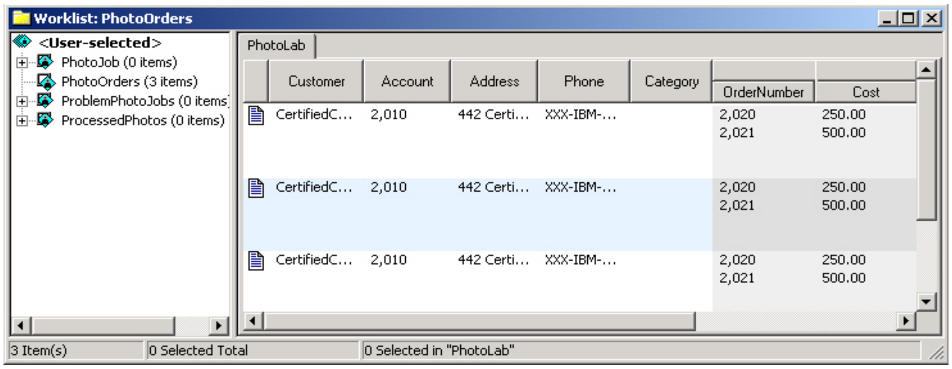
Worklists: <User-selected>

<User-selected>
PhotoJob (0 items)
PhotoOrders (3 items)
ProblemPhotoJobs (0 items)
ProcessedPhotos (0 items)

Figure 12–10 *Windows Client Worklist Counts*

15. ___ The **PhotoOrders** worklist should list three items, (see Figure 12–11).

The items passed directly through the PhotoJob collection node and were sent on to the next work node (*PhotoProcessing*) immediately because only folders are held in a collection work node.



Worklist: PhotoOrders

<User-selected>
PhotoJob (0 items)
PhotoOrders (3 items)
ProblemPhotoJobs (0 items
ProcessedPhotos (0 items)

PhotoLab

Customer	Account	Address	Phone	Category	OrderNumber	Cost
CertifiedC...	2,010	442 Certi...	XXX-IBM-...		2,020 2,021	250.00 500.00
CertifiedC...	2,010	442 Certi...	XXX-IBM-...		2,020 2,021	250.00 500.00
CertifiedC...	2,010	442 Certi...	XXX-IBM-...		2,020 2,021	250.00 500.00

3 Item(s) | 0 Selected Total | 0 Selected in "PhotoLab"

Figure 12–11 *PhotoOrder worklist displaying three items.*

When items were imported into the PhotoLab item type, the auto-link definition in PhotoLab should have created a folder in the MyPhotoWork item type. This folder can also be added to the document routing process.

16. ___ Select **Search** on the Client for Windows.

17. ___ Select **Basic**.

18. ___ On the *Basic Search* screen, select **MyPhotoWork** for the item type.

19. ___ Select **OK**.

20. ___ A list of defined folders for the item type should be displayed.

21. ___ Highlight **Certified Customer** the folder automatically created during the previous import.

22. ___ Using the **Action Menu**, select **Process** and then **Start on**.

23. ___ Select **ProcessPhotos** as the process.

24. ___ Select **Start**.

25. ___ Re-open the **Worklists**.

26. ___ Open the **PhotoOrders Worklist**.

    The Worklist now contains the items placed on the process during import into PhotoLab and a MyPhotoWork folder. Notice the folder passed through the collection because the folder already contained three items and the collection resume list for the item type states 2 required.

27. ___ Now import a single file using the **Photolab** item type. Do not start the file on a process.

28. ___ Once imported do another **Basic Search** using the **MyPhotoWork** item type to find the new folder.

29. ___ Start this folder on the **ProcessPhotos** process.

30. ___ Re-open the **Worklists**.

31. ___ The PhotoJob Worklist representing the PhotoJob collection work node should now contain one folder item of MyPhotoWork item type.

32. ___ Opening this folder will list the single file that was imported.

Working Items in a Process

1. ___ Highlight one of the items listed in a worklist.

2. ___ Select the **Actions** menu, then the **Process** menu. Table 12–6 on page 389

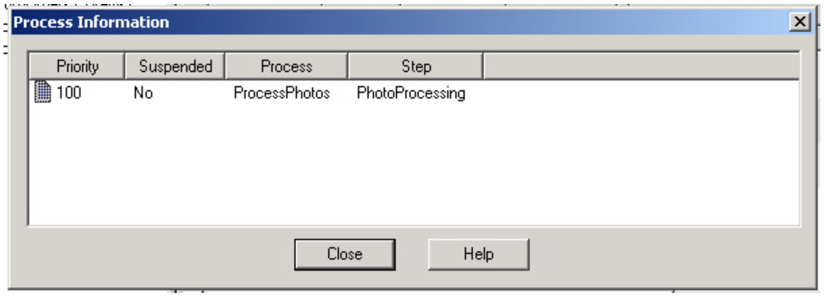
lists the process actions.

Table 12–6 *Client for Windows document routing process actions*

Process Action	Default Purpose for the Action
Start on	Will display a list of document processes for which the item can be assigned. This lets you start an item on another process without removing the item from the current process. (Part of the ad-hoc document routing process.)
Change	Will display a list of available document routing processes that the selected item can be assigned. This removes the item from the current process.
Continue	One of the predefined acceptable actions defined for this step in the process. In the ProcessPhotos process *continue* moves the item onto the next work node. Any text can be used for an action in the process.
Escalate	One of the predefined acceptable actions defined for this step in the process. In the ProcessPhotos process *escalate* is used to re-route the work package referencing the item to a work node other than the normal next step handled by continue. Any text can be used for an action in the process.
Remove from	Delete the item from the process. The item remains in the library system.
Priority	Alter the priority for the selected item. The larger the number the lower the priority for the item.
Suspend	Interrupt the process for the item, temporarily suspending the item.
Activate	Reactivate an item that has been suspended.
Info.	Display process status information for the selected item.

3. ___ Select **Info.** to display the process information for the item, (see Figure 12–12).

.



Priority	Suspended	Process	Step
100	No	ProcessPhotos	PhotoProcessing

Figure 12–12 *Process information for select item in a worklist*

The process information for the item shows the work node or process step for where the item resides and if the item has been suspended.

4. ___ Highlight one of the items listed in a the PhotoOrders worklist and select **Priority**.

Notice the available actions will be different if selecting a document or file started on the process directly when imported versus an item contained in a folder that was started on the process. An item contained in a folder on the worklist may only have the Start on and Info actions available. This is because when the folder was placed on the process, the folder represents the work package and the files contained in the folder are treated as a single process entity.

5. ___ Change the **Priority** to **50** in order to give it a higher priority.

6. ___ For the same item now select **Suspend**. Set the **suspend** time to **four minutes.**

This will provide an opportunity to see what the client does with items that are reactivated. Notice the suspended item remains in the list of items in the worklist.

7. ___ For the same item, select **Start** on and select the **ProblemPhotosJob**, (see Figure 12–13 on page 391).

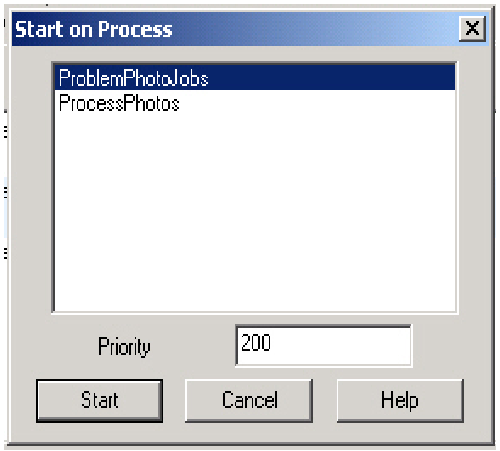


Figure 12–13 *Document routing start a new process screen*

This will start a new work package for the referenced item on the new process. The item on the existing process remains. If **Info** is selected again, all the work packages on the different processes for the referenced item will be listed.

8. ___ Highlight one of the items listed in the PhotoOrders worklist and select **Continue**.

This should have removed the item from the ProcessOrders worklist and moved it to the ProcessedPhotos worklist representing the next work node in the process. ProcessedPhotos should now have one item listed.

9. ___ Highlight one of the items listed in the PhotoOrders worklist and select **Escalate**.

This should have removed the item from the ProcessOrders worklist and moved it to the ProblemPhotoJobs worklist. ProblemPhotoJobs should now have at least one item listed. This was the exception process entered into the ProcessOrders document routing process.

10. ___ Highlight one of the items listed in ProcessedPhotos and select **Continue**.

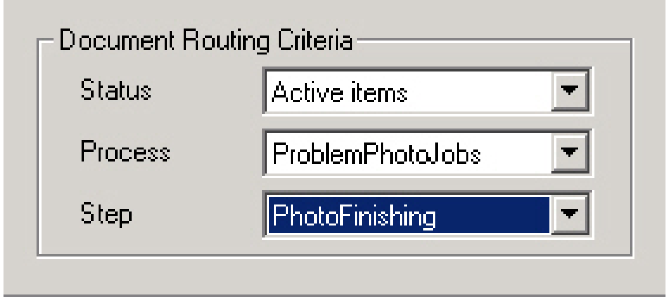
Notice that Escalate is not listed as an action because it was not defined as a valid action for items leaving the Photo Finishing work node. Once items leave the Photo Finishing work node, the next step is the end of the process.

11. ___ Highlight one of the items listed in the ProblemPhotoJobs worklist and select **Escalate**.

This should have removed the item from the ProblemPhotoJobs worklist and moved it to the end of the process.

Searching for Items on a Process

Along with the ability to take action on process items, the Client for Windows search facility provides support for searching for items in a process based on its status, process, or step in the process. Figure 12–14 contains the captured area of the basic search screen containing the fields used for searching for items based on document routing criteria.



Document Routing Criteria

Status: Active items

Process: ProblemPhotoJobs

Step: PhotoFinishing

Figure 12–14 *Document routing search criteria from the basic search screen*

Status allows a search to be performed for all items, suspended items, or active items. **Process** provides for selecting the defined processes the user can access. **Step** allows the user to select the work node or step for the selected process. Try performing some searches using the above fields.

Client for Windows Viewer

This section will point out some of the features included with the Client for Windows document and image viewer. The viewer relies on standard industry conversion tools to enable different document and image formats to be displayed and manipulated. As mark-ups are being done on the displayed items, these annotations will be saved in the document item type ICMAnnotations part. Information added to the notelog for the item will be saved in the document item type ICMNotelog part.

1. ___ Perform a basic search in the Client for Windows.

2. ___ From the listed items select and open one of the imported images.

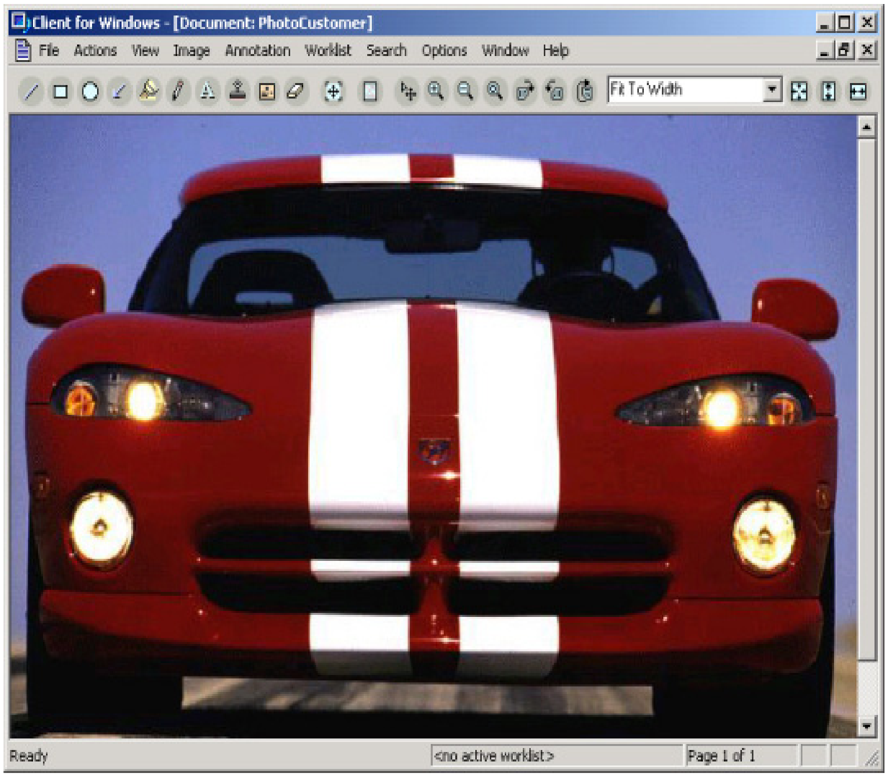

Client for Windows - [Document: PhotoCustomer]
File Actions View Image Annotation Worklist Search Options Window Help
Fit To Width
Ready
<no active worklist>
Page 1 of 1

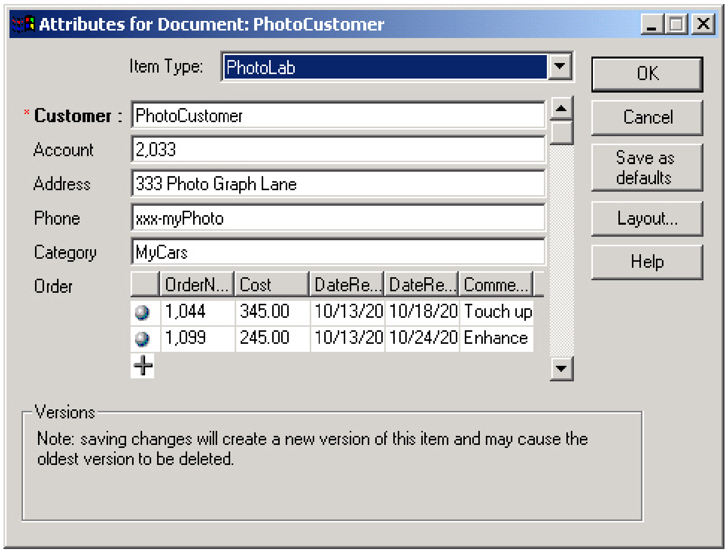
Figure 12–15 *Content Manager Windows Client Viewer*

3. ___ Figure 12–15 displays an image in the client viewer, along with the annotation tool bar shown at the top.

Attributes for Displayed Image

1. ___ Select the **Action** menu.

2. ___ Select **Attributes** to display the attributes for the displayed image, (see Figure 12–16).



Attributes for Document: PhotoCustomer

Item Type: PhotoLab

* **Customer :** PhotoCustomer

Account 2,033

Address 333 Photo Graph Lane

Phone xxx-myPhoto

Category MyCars

Order

	OrderN...	Cost	DateRe...	DateRe...	Comme...
●	1,044	345.00	10/13/20	10/18/20	Touch up
●	1,099	245.00	10/13/20	10/24/20	Enhance
+					

Note: saving changes will create a new version of this item and may cause the oldest version to be deleted.

Figure 12–16 *Attributes for the displayed or selected image*

3. ___ Notice in Figure 12–16 the child level attributes listed for order.

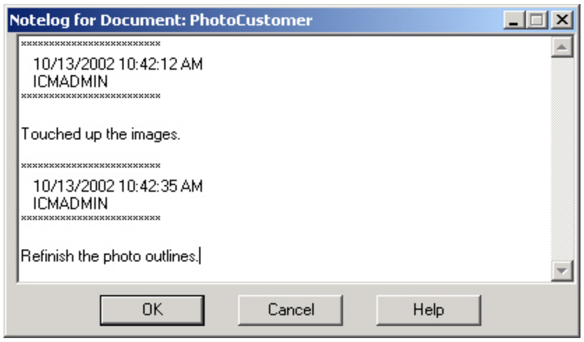
4. ___ Select the plus sign **(+)** and add another row of multi-valued attributes. Type your own information into the fields.

5. ___ Select **OK** to save the attributes.

Notelog for Displayed Image

1. ___ Select the **Action** menu.

2. ___ Select **Notelog** to display the attributes for the displayed image, (see Figure 12–17 on page 395).



```
****************************
  10/13/2002 10:42:12 AM
  ICMADMIN
****************************

Touched up the images.

****************************
  10/13/2002 10:42:35 AM
  ICMADMIN
****************************

Refinish the photo outlines.
```

Figure 12–17 *Notelog for the displayed image or selected image*

3. ___ Type an entry in the notelog like **Refinished the photo outlines**.

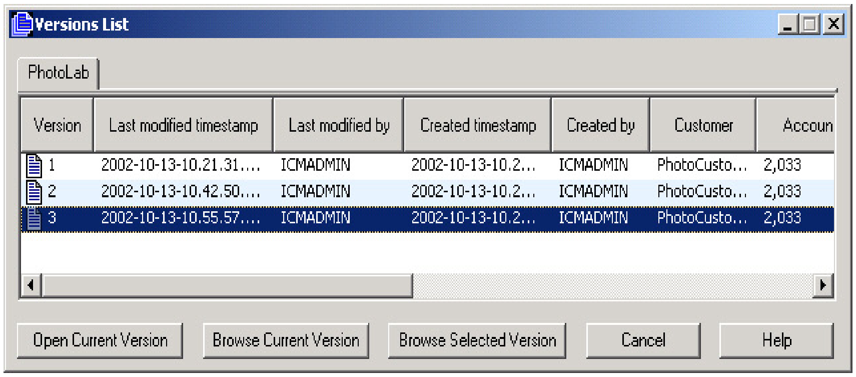
4. ___ Select **OK** to save the notelog.

5. ___ Each time the notelog is displayed an additional time stamp is added.

Versions for the Displayed Image

1. ___ Select the **Action** menu.

2. ___ Select **Versions List** to display the attributes for the displayed image, (see Figure 12–18).



Version	Last modified timestamp	Last modified by	Created timestamp	Created by	Customer	Accoun
1	2002-10-13-10.21.31....	ICMADMIN	2002-10-13-10.2...	ICMADMIN	PhotoCusto...	2,033
2	2002-10-13-10.42.50....	ICMADMIN	2002-10-13-10.2...	ICMADMIN	PhotoCusto...	2,033
3	2002-10-13-10.55.57....	ICMADMIN	2002-10-13-10.2...	ICMADMIN	PhotoCusto...	2,033

Figure 12–18 *Version list for the displayed or selected image*

3. ___ You can select any of the listed versions to work with older versions. The version list will continue to add versions of the item until the maximum number specified in the item type has been reached. Once reached the oldest version is deleted.

Note: If an item is re-indexed or re-classified to another item type, the old versions do not accompany the item to the new item type classification. The older versions are removed.

4. ___ Select **Cancel** to close the version list.

Marking up the Displayed Image

Use the following list to assist in marking up the displayed image or document. Added annotations do not alter the original image, but are saved separately as ICMAnnotation parts and used to overlay the image or document when displayed.

Line tool for drawing a ***line*** between any two points on the displayed image or document.

For placing a ***rectangular box*** around portions of the displayed image or document.

For drawing a ***circle*** or oval around portions of the displayed image or document.

For adding ***arrows*** to the displayed image or document.

The ***highlighter*** is used to add rectangular highlights to the displayed image or document.

The ***pen*** is used to draw free-form lines on the displayed image or document.

For adding ***text*** annotations to the displayed image or document.

The ***stamp*** is used to add an annotation that resembles a rubber stamp. The stamp properties allow you to change the stamp text and affects.

Add ***sticky notes***, with entered text, of any size to the displayed image or document.

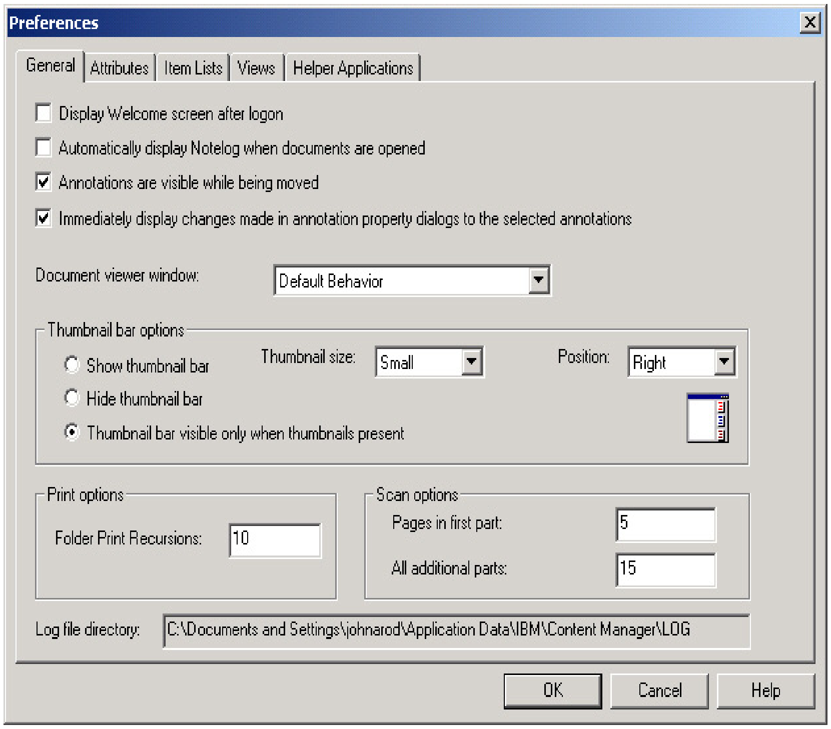
Client for Windows Preferences

This section will point out additional preferences that can be set for the Client for Windows.

1. ___ Select **Options**.
2. ___ Select **Preferences**.

General Preferences

1. ___ Select **General**.



Preferences

General | Attributes | Item Lists | Views | Helper Applications

☐ Display Welcome screen after logon
☐ Automatically display Notelog when documents are opened
☑ Annotations are visible while being moved
☑ Immediately display changes made in annotation property dialogs to the selected annotations

Document viewer window: Default Behavior

Thumbnail bar options
○ Show thumbnail bar
○ Hide thumbnail bar
● Thumbnail bar visible only when thumbnails present
Thumbnail size: Small
Position: Right

Print options
Folder Print Recursions: 10

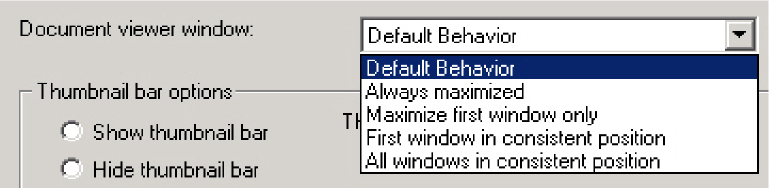
Scan options
Pages in first part: 5
All additional parts: 15

Log file directory: C:\Documents and Settings\johnarod\Application Data\IBM\Content Manager\LOG

Figure 12–19 *Client for Windows general preferences*

2. ___ Deselect the **Display Welcome screen after logon**, (see Figure 12–19). This will cause the client window to be displayed without icons.
3. ___ Select **Thumbnail bar visible only when thumbnails present**.
4. ___ Select **Right** for the thumbnail position.

5. ___You can also alter the default display action for the document viewer. (see Figure 12–20).



Document viewer window: Default Behavior

Thumbnail bar options

○ Show thumbnail bar

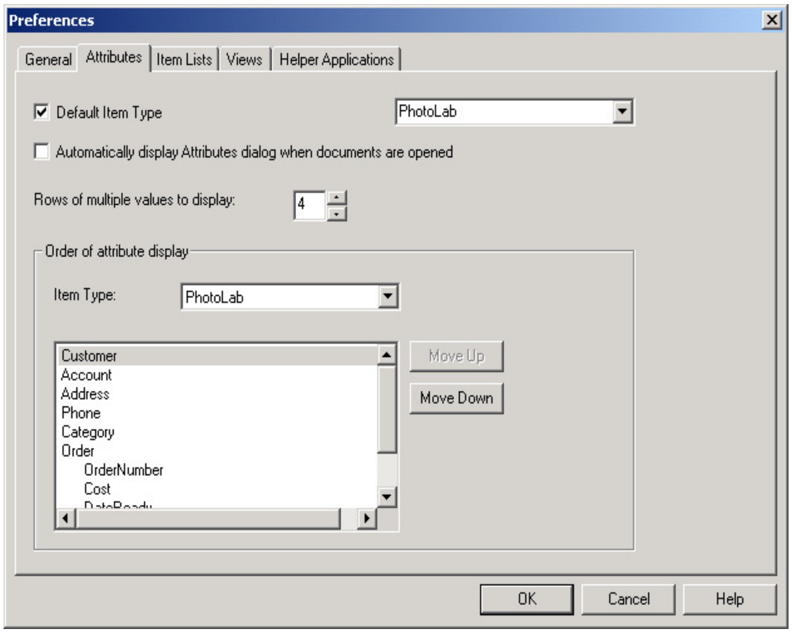
○ Hide thumbnail bar

Default Behavior
Always maximized
Maximize first window only
First window in consistent position
All windows in consistent position
Th

Figure 12–20 *Document viewer default display options*

Attributes Preferences

1. ___ Select the **Attributes** tab, (see Figure 12–21).
2. ___ Set the *Default item type* to **PhotoLab**.
3. ___ Set the *Rows of multiple values to display* to **4**.



Preferences

☑ Default Item Type: PhotoLab

□ Automatically display Attributes dialog when documents are opened

Rows of multiple values to display: 4

Order of attribute display

Item Type: PhotoLab

Customer
Account
Address
Phone
Category
Order
    OrderNumber
    Cost
    DateReady

Figure 12–21 *Client for Windows attribute preferences*

On the *Attributes* preference screen you can also alter the order of the attributes to be displayed. For the PhotoLab, **reorder** some of the attributes for the Order. Notice that the attributes for the Child Component cannot be moved outside of the Child Component definition.

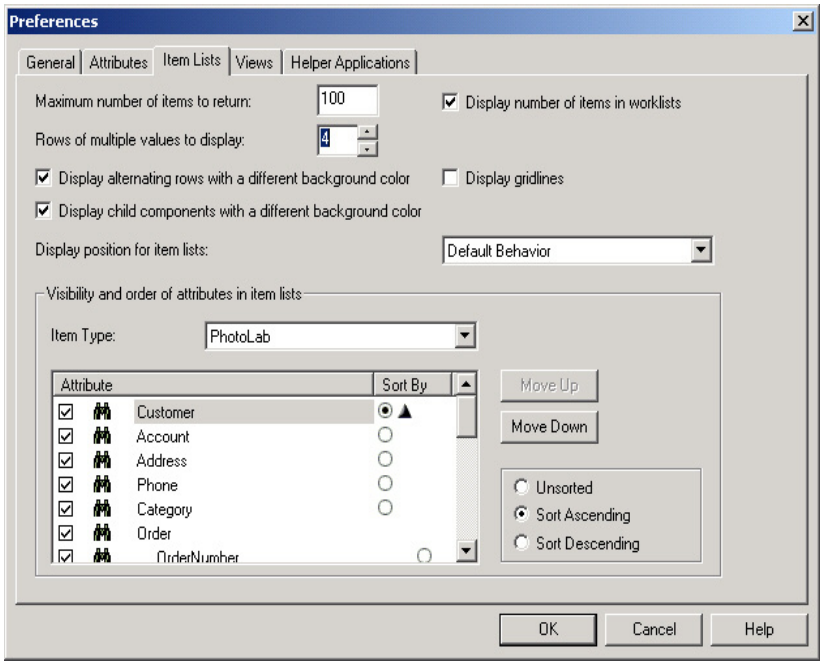
Item Lists Preferences

1. ___ Select the **Item Lists** tab, (see Figure 12–22).

2. ___ Set the *Rows of multiple values to display* to **4**

3. ___ Select **Display child components with a different background color**.

4. ___ Set the **Display number of items in work lists**.



Preferences

Maximum number of items to return: 100

☑ Display number of items in worklists

Rows of multiple values to display: 4

☑ Display alternating rows with a different background color

☐ Display gridlines

☑ Display child components with a different background color

Display position for item lists: Default Behavior

Visibility and order of attributes in item lists

Item Type: PhotoLab

Attribute	Sort By
☑ Customer	● ▲
☑ Account	○
☑ Address	○
☑ Phone	○
☑ Category	○
☑ Order	
☑ OrderNumber	○

○ Unsorted

● Sort Ascending

○ Sort Descending

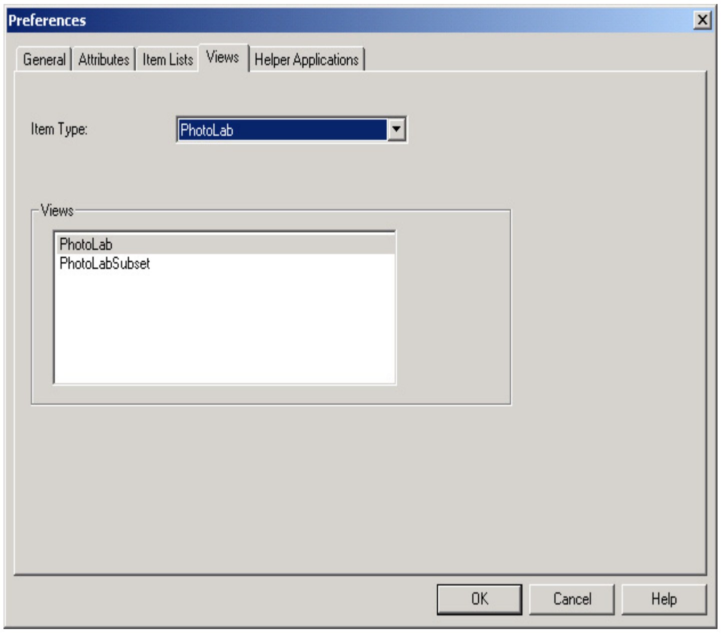
Figure 12–22 *Client for Windows item lists preferences*

5. ___ Look at the **Visibility and order of attributes in item lists**. For the PhotoLab, you can deselect attributes that you do not want displayed and sort the contents of the displayed attributes.

View Preferences

Lists the different views available for the item type selected, see Figure 12–23 on page 400.

1. ___ Select **Views** tab.



Item Type: PhotoLab

Views
PhotoLab
PhotoLabSubset

Figure 12–23 *Client for Windows view preferences*

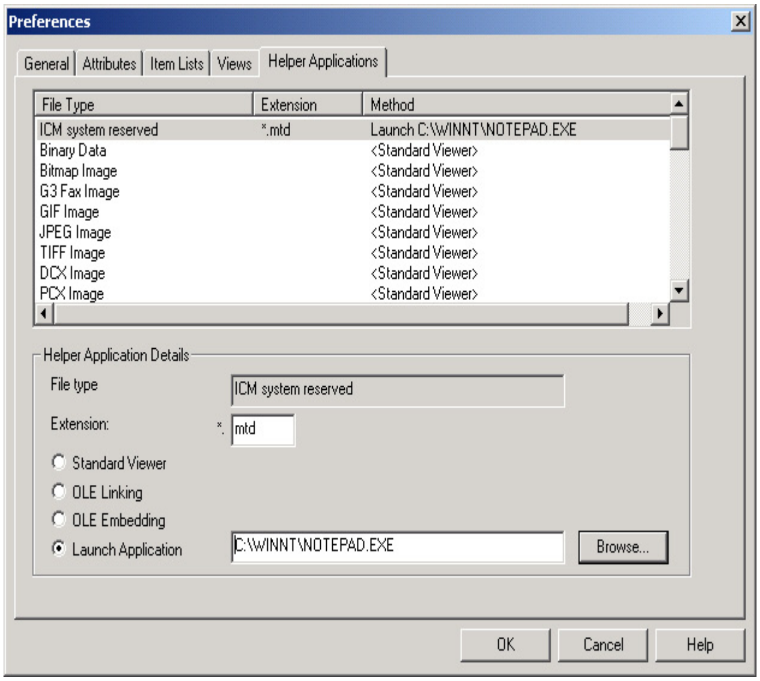
Helper Applications

The helper applications screen allows one to identify to the Client for windows how defined MIME types or file extensions should be handled.

1. ___ Select **Helper Applications** tab.

2. ___ Type **mtd** in the Extensions field. This is the MIME type added during the document modeling section of this guide.

3. ___ Select **C:\WINNT\NOTEPAD.EXE** for the Launch Application. This will cause notepad to be launch when ever a item with *.mtd is selected in the Client for Windows, (see Figure 12–24 on page 401).



File Type	Extension	Method
ICM system reserved	*.mtd	Launch C:\WINNT\NOTEPAD.EXE
Binary Data		<Standard Viewer>
Bitmap Image		<Standard Viewer>
G3 Fax Image		<Standard Viewer>
GIF Image		<Standard Viewer>
JPEG Image		<Standard Viewer>
TIFF Image		<Standard Viewer>
DCX Image		<Standard Viewer>
PCX Image		<Standard Viewer>

Helper Application Details

File type: ICM system reserved

Extension: *. mtd

○ Standard Viewer

○ OLE Linking

○ OLE Embedding

● Launch Application C:\WINNT\NOTEPAD.EXE

Figure 12–24 *Client for Windows Helper Applications preferences*

4. ___ Select **OK** to save the modified preferences.

With the preferences altered, you may want to redo some of the scenarios in the previous sections to see how the Client for Windows has changed.

Summary

This section has been used to provide a visual example of how the Content Manager enhancements like the new data model, text search, and document routing are used in the Client for Windows. Table 12–7 lists the data model features that the Client for Windows supports.

Table 12–7 *Data Model features supported by the Client for Windows*

logonData Model Element	Supported
Attribute	Yes[1]
Attribute Group	No
Root Component	Yes
Child Component	One level only
Item[2]	No
Resource Item[2]	No
Document[2]	Yes
Document Part[2]	Yes
Versions	Yes
Media Object Class	Yes
Item Type Subset[3]	Yes
Semantic Type	Document and folder only
MIME Type	Yes
Links	Folder only
References	No
Foreign Keys	No

Notes:
1. Except for BLOB and CLOB types.
2. Item Type Classification
3. Referred to as, *views* in the Client for Windows.

CHAPTER 13

eClient

- Importing Using Item Types
- Searching for Items
- Using Text Search
- Using Document Routing

In this chapter, the Content Manager eClient will be used to demonstrate the use of the new data model and document routing features of Content Manager. Along with importing items into Content Manager using the eClient, this section will point out eClient enhancements such as the Viewer Applet, check in and check out, document routing, folders, eClipboard, version support, and direct object retrieval. The focus of this chapter is strictly on the support eClient provides for Content Manager and detail on eClient interactions with Enterprise Information Portal function will not be covered. The *IBM Certification Solutions Expert (CSE) - IBM Content Manager Version 8 Certification Exam 442* contains questions on how the eClient works with Content Manager

Overview

Content Manager eClient version 8.1 provides a significant enhancement in the way documents and images are rendered and delivered to the browser client. With the normal eClient browser process, items selected in a search results hit list are retrieved from the Content Manager Resource Manager through the eClient application server. This can provide a bottle neck and performance drain as users work with displayed images requiring process support from the eClient application server. With the new design, items selected in the search results hit list can be retrieved directly from the Content Manager Resource Manager if the new Viewer Applet is being used. The Viewer Applet interacts directly with the Resource Manager (see Figure 13–1) to retrieve the desired object and then handles the rendering of the object as users perform actions on the displayed object. The customer has the option of which process to use. They can continue to use the client browser with images posted from the eClient application server, or use the new Viewer Applet. The setting is made for each MIME type in the *IDMadminDefaults.properties* file.

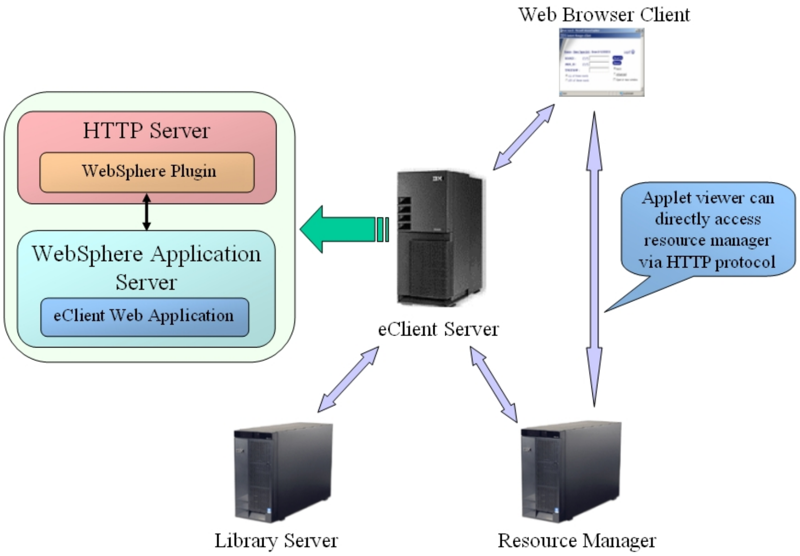


Figure 13–1 *Enhanced eClient architecture*

Along with the Viewer Applet, eClient version 8.1 provides the following enhancements for interacting with Content Manager version 8.1.

- Launching search results in separate windows
- Importing and deleting of documents and images
- Check Out and In support for documents and images
- Re-indexing of documents and images
- Support for creating folders
- eClipboard so that items can be copied into folders and across processes
- Document version support
- Support for Content Manager document and notelogs
- Support for the new item type document model in Content Manager version 8.1
- Support for Content Manager version 8.1 document routing
- and paging support in the eClient so the first page can be displayed prior to all of the search results being retrieved.

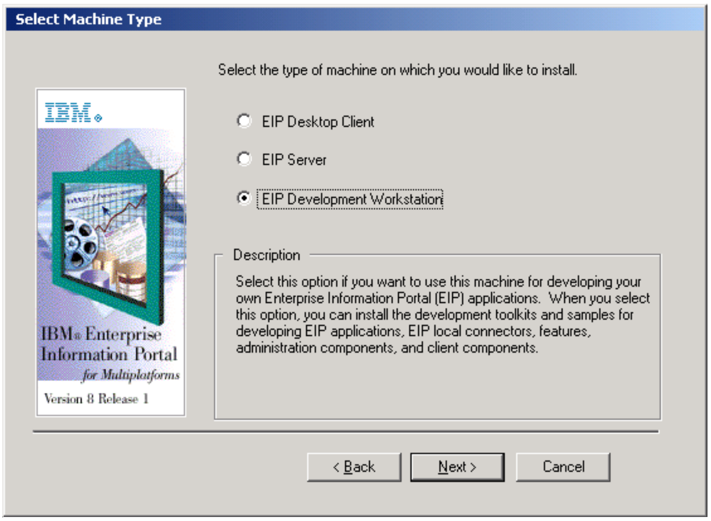
Many of these enhancements will be cover in this section of the study guide.

Before the enhancements of the eClient can be demonstrated, the Enterprise Information Portal connector for Content Manager version 8.1 must be installed. Once completed, the eClient can then be installed and configured. Other than the connector for Content Manager version 8.1, this guide will not discuss any of the enhancements made to the Enterprise Information Portal (EIP).

Install Content Manager V8 Connector

The focus of this guide is the content on the *IBM Certified Solutions Expert (CSE) - IBM Content Manager Version 8 (442)* exam. This exam covers the concepts and skills required to install and administrate a Content Manager system using the Client for Windows and/or eClient. The content of Enterprise Information Portal for Multiplatforms (EIP) is not represented on this exam. Because of this, the focus of this section will be to install the Enterprise Information Portal for Multiplatforms connector that eClient requires for connecting to a Content Manager server. The connector can be installed on the local server or a remote machine. If on a remote machine, an RMI server will be required for connecting to the Content Manager server. For the purposes of this guide, the assumption is made that a single machine is being used and will provide the steps for installing the connector on the Content Manager server.

1. ___ Start the Enterprise Information Portal installation program.
2. ___ Select **Accept** on the License Agreement.
3. ___ Select **Next** on the EIP information panel.



Select the type of machine on which you would like to install.

○ EIP Desktop Client

○ EIP Server

● EIP Development Workstation

Description

Select this option if you want to use this machine for developing your own Enterprise Information Portal (EIP) applications. When you select this option, you can install the development toolkits and samples for developing EIP applications, EIP local connectors, features, administration components, and client components.

Figure 13–2 *EIP Machine Type selection screen*

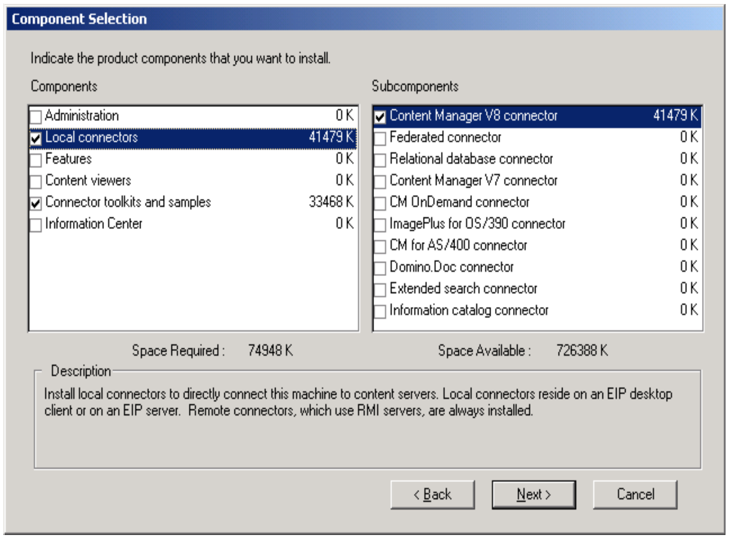
4. ___ Select **EIP Development Workstation** on the Select Machine Type (see Figure 13–2).

5. ___ Take the default **C:\CMBROOT** for the installation directory.

   Notice also that c:\Program Files\IBM\Cmgmt will be used as the default location for the common configuration files shared between Content Manager and EIP.

6. ___ Select **Next**.

7. ___ Select **Local Connectors** on the *Component Selection* screen (see Figure 13-3).



Component Selection

Indicate the product components that you want to install.

Components

□ Administration	0 K
☑ Local connectors	41479 K
□ Features	0 K
□ Content viewers	0 K
☑ Connector toolkits and samples	33468 K
□ Information Center	0 K

Subcomponents

☑ Content Manager V8 connector	41479 K
□ Federated connector	0 K
□ Relational database connector	0 K
□ Content Manager V7 connector	0 K
□ CM OnDemand connector	0 K
□ ImagePlus for OS/390 connector	0 K
□ CM for AS/400 connector	0 K
□ Domino.Doc connector	0 K
□ Extended search connector	0 K
□ Information catalog connector	0 K

Space Required : 74948 K

Space Available : 726388 K

Description

Install local connectors to directly connect this machine to content servers. Local connectors reside on an EIP desktop client or on an EIP server. Remote connectors, which use RMI servers, are always installed.

Figure 13-3 *EIP installation component selection screen*

8. ___ Select the **Content Manager V8 connector** subcomponent.

9. ___ Make sure no other items are selected under the *subcomponents* area.

10. ___ Select the **Connector toolkits and samples** component.

11. ___ Select the **Content Manager v8 connector** subcomponent.

12. ___ Make sure no other items are selected under the *subcomponents* area.

13. ___ Select **Next**.

14. ___ Take the system defaults on the *Specify RMI Host Name and Port Number* screen.

15. ___ Select **Next**.

16. ___ Take the defaults on the *System Configuration* screen.

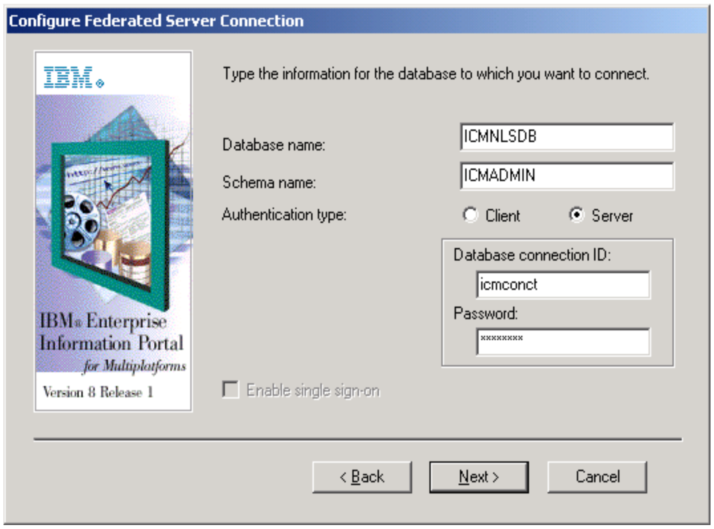
17. ___ Select **Next**.

18. ___ Use the values in Table 13–1 to verify and enter the required information on the *Configure Federated Server Connection* and *Configure Content Manager V8 Server Connection* installation screens.

Table 13–1 *Configure federated server connection values*

Field	Value
Database	ICMNLSDB
Schema Name	ICMADMIN
Server	Server
Database Connection ID	icmconct
Password	password

19. ___ The Configure Federated Server Connection screen should resemble Figure 13-4.



Configure Federated Server Connection

Type the information for the database to which you want to connect.

Database name: ICMNLSDB

Schema name: ICMADMIN

Authentication type: ○ Client ● Server

Database connection ID: icmconct

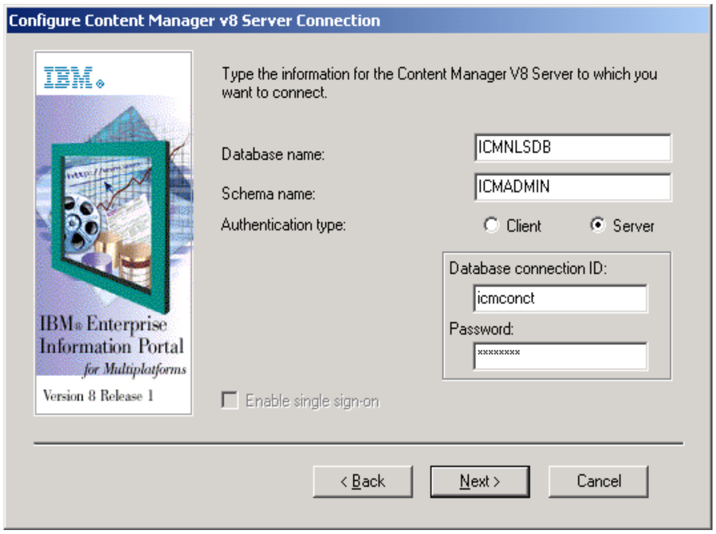
Password: ********

□ Enable single sign-on

Figure 13-4 *EIP configure federated server connection*

20. ___ Select **Next**.

21. ___ The *Configure Content Manager V8 Server Connection* screen should resemble Figure 13-5.



Configure Content Manager v8 Server Connection

Type the information for the Content Manager V8 Server to which you want to connect.

Database name: ICMNLSDB

Schema name: ICMADMIN

Authentication type: ○ Client ● Server

Database connection ID: icmconct

Password: ********

□ Enable single sign-on

Figure 13-5 *Configure Content Manager V8 Server Connection*

22. ___ Select **Next**.

23. ___ Select **Next** on the *Start Copying Files* screen.

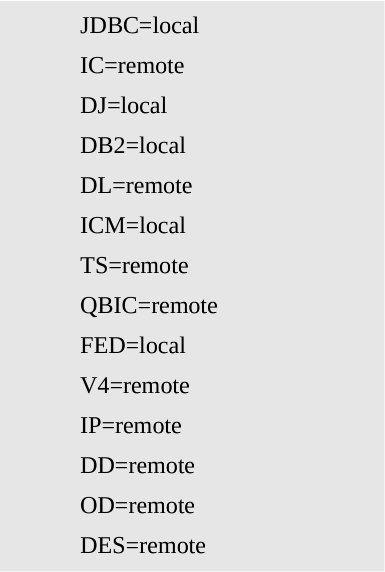
A message window might be displayed indicating that the Content Manager database will be configured for use by both Content Manager and EIP. If displayed, select **OK** to proceed.

24. ___ Select **Yes, I want to restart my computer now** when the installation is completed.

EIP Connector Configuration File

With the connector installed on the server, the EIP connector configuration file should not need modification. If multiple connectors had been installed or the connector had been installed on a remote machine, the ***cmbcs.ini*** connector configuration file may need to be updated to reflect whether the server is local or remote, (see Figure 13–6 for an example of the *cmbcs.ini* file). Check the ***cmbcs.ini*** file to make sure the *ICM=Local* setting for the Content Manager Version 8 connector is set to **local**. Notice that the JDBC, DB2, and FED are also set to **local** indicating installation with the database on the local server.

1. ___ Open file **C:\Program Files\IBM\Cmgmt\cmbcs.ini**.
2. ___ Review the connector settings.
3. ___ Make sure **ICM=local**.
4. ___ Close the file.



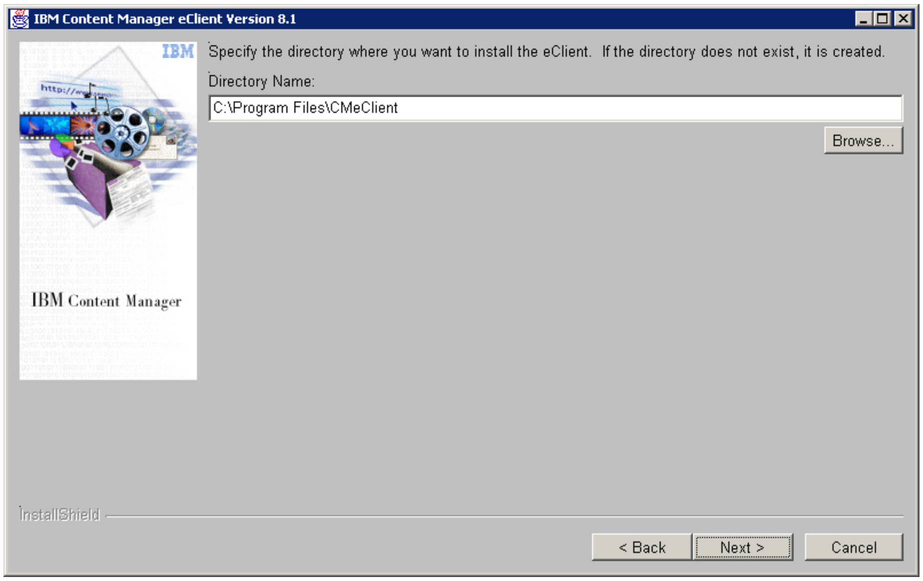
```
JDBC=local
IC=remote
DJ=local
DB2=local
DL=remote
ICM=local
TS=remote
QBIC=remote
FED=local
V4=remote
IP=remote
DD=remote
OD=remote
DES=remote
```

Figure 13–6 *Contents of the cmbcs.ini configuration file*

Install Content Manager eClient

With the Content Manager server already installed and operational, and the EIP connector for Content Manager Version 8 installed, eClient can be installed without altering prerequisite software. If this was a remote machine running WebSphere Application Server (AE) you would need to make sure that the web services had been started. The following steps assume that you are using WebSphere Application Server (AEs) that is shipped with the Content Manager media.

1. ___ Start **x:\WIN\setup.exe**.
2. ___ Select **Next** on the eClient Welcome screen.
3. ___ Select **English** for the install language and select **Next**.
4. ___ Take the default **C:\Program Files\CMeClient** Directory Name on the screen shown in Figure 13–7.



IBM Content Manager eClient Version 8.1

Specify the directory where you want to install the eClient. If the directory does not exist, it is created.

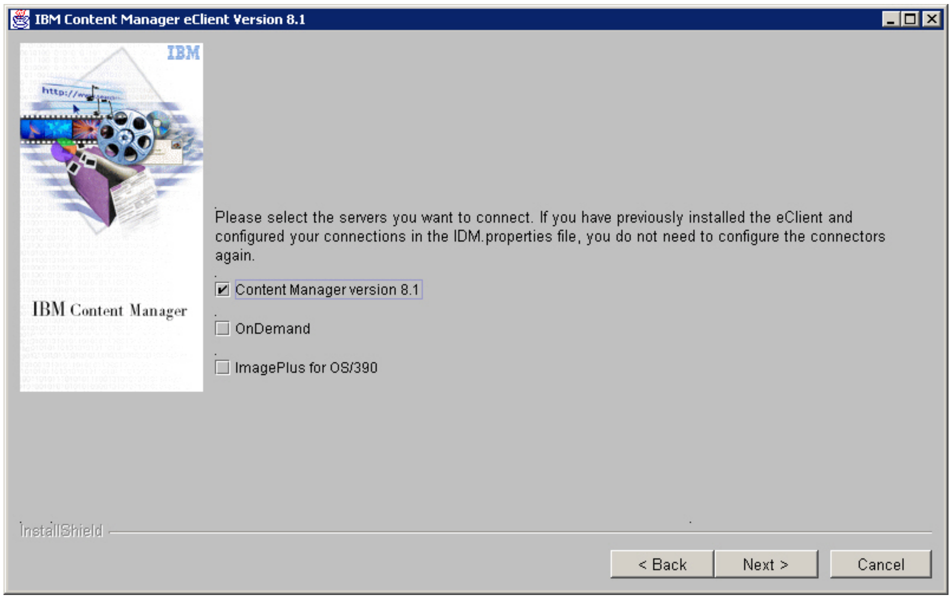
Directory Name:

C:\Program Files\CMeClient

Figure 13–7 *Content Manager installation directory*

5. ___ Select **Next**.
6. ___ Select **Next** on the installation information screen.
7. ___ On Confirmation panel, select **Next**.

8. ___ Select **Content Manager Version 8.1** on the server selection screen shown in Figure 13-8.



Please select the servers you want to connect. If you have previously installed the eClient and configured your connections in the IDM.properties file, you do not need to configure the connectors again.

☑ Content Manager version 8.1

□ OnDemand

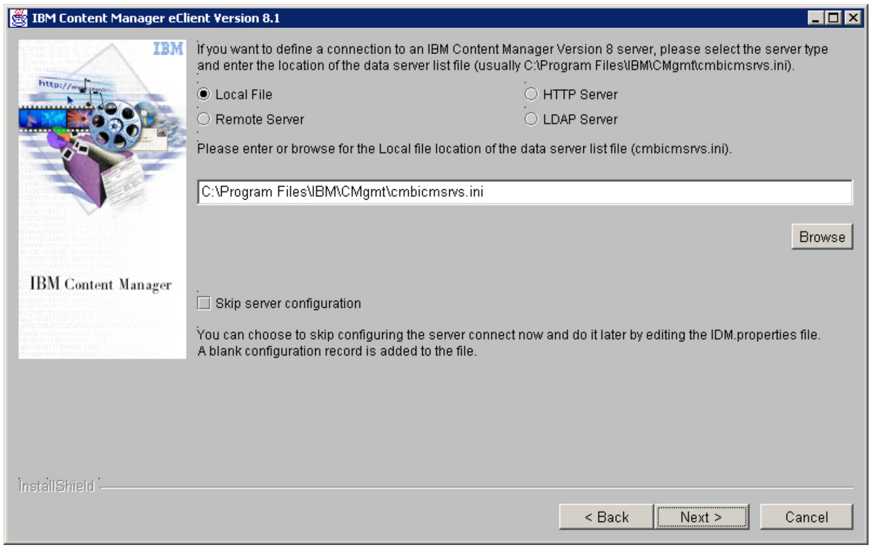
□ ImagePlus for OS/390

Figure 13-8 *eClient installation server selection screen*

9. ___ Select **Next**.

10. ___ On the *Content Manager Server configuration file selection* screen, (see Figure 13-9 on page 413) select the location of the file on your machine. The default should be **C:\Program Files\IBM\CMgmt\cmbicmsrvs.ini**.

    Note the server configuration file can reside on the local machine, an http server, remote server or LDAP server. This step can be skipped, but the eClient *IDM.Properties* file will need to be edited with the location of the server.



IBM Content Manager eClient Version 8.1

If you want to define a connection to an IBM Content Manager Version 8 server, please select the server type and enter the location of the data server list file (usually C:\Program Files\IBM\CMgmt\cmbicmsrvs.ini).

● Local File ○ HTTP Server
○ Remote Server ○ LDAP Server

Please enter or browse for the Local file location of the data server list file (cmbicmsrvs.ini).

C:\Program Files\IBM\CMgmt\cmbicmsrvs.ini

□ Skip server configuration

You can choose to skip configuring the server connect now and do it later by editing the IDM.properties file. A blank configuration record is added to the file.

Figure 13-9 *Configure Content Manager version 8.1 connection*

11. ___ Select **Next** to complete the eClient installation and deploy the eClient in WebSphere Application Server (AEs).

12. ___ Deploying the eClient may take a little while, so be patient as status screens are not necessarily displayed.

13. ___ Notice on the eClient installation completion screen the following message stating to complete the configuration and startup for the eClient running on WebSphere Application Server (AEs).

> **Note:** To start WebSphere Advanced Single Server with the integrated eClient application installed, execute **startIDMAES.bat** which is located in the eClient save directory.

14. ___ Select **Finish**.

15. ___ Open a **Command Line** window.

16. ___ Run **C:\Program Files\CMeClient\Save\startIDMAES.bat** to complete the setup. The process will use the IDM_ICM.xml file located in the default C:\Program Files\ibm\Cmgmt\ directory to complete the setup of the ICM_Server default server for eClient. Figure 13–10 shows the command line output from this process.

```
Application Server Launcher
Copyright (C) IBM Corporation, 2001

The configuration file was accepted as:
   C:\Program Files\IBM\Cmgmt\IDM_ICM.xml
Using the single available node or the localhost node.
Using the server "ICM_Server".
Initiating server launch.
Loaded domain "WebSphere Administrative Domain".
Selected node "edmbeta".
Selected server "ICM_Server".
WSPL0065I: Initiated server launch with process id 328.
Time mark: Wednesday, October 30, 2002 8:57:43 PM CST
Waiting for the server to be initialized.
Time mark: Wednesday, October 30, 2002 8:57:50 PM CST
Initialized server.
Waiting for applications to be started.
Time mark: Wednesday, October 30, 2002 8:58:16 PM CST
Started applications.
WSPL0057I: The server ICM_Server is open for e-business.
Please review the server log files for additional information.
Standard output: C:\WebSphere\AppServer/logs/ICM_stdout.log
Standard error: C:\WebSphere\AppServer/logs/ICM_stderr.log
```

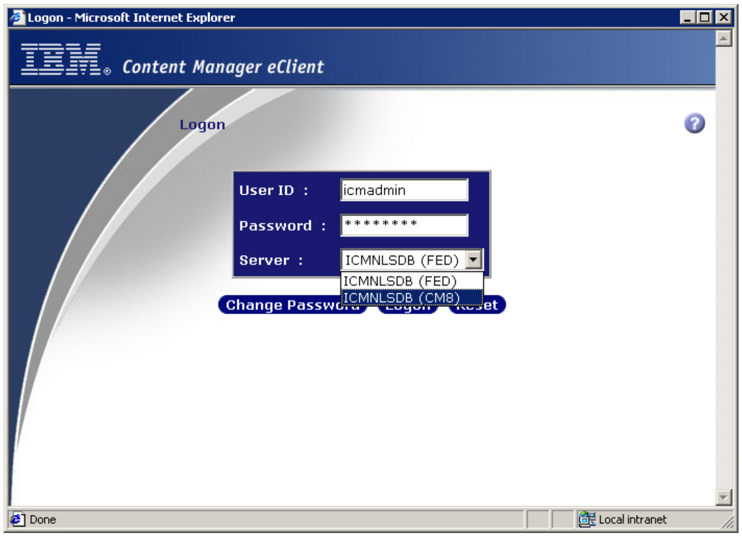
Figure 13–10 *Command line output from running startIDMAES.bat*

The eClient has now completed the installation and configuration in WebSphere Application Server (AEs).

17. ___ Open an **Internet Explorer** window.

18. ___ Type **http://localhost/eClient81/IDMInit** as the URL, press **Enter**.

19. ___ If installation and deployment were successful the eClient logon screen shown in Figure 13–11 should be displayed.



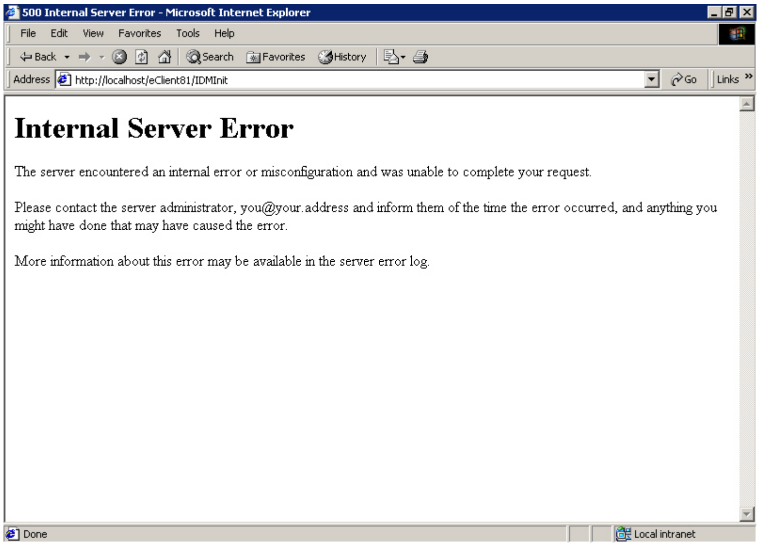
User ID : icmadmin

Password : ********

Server : ICMNLSDB (FED)

Figure 13–11 *eClent logon screen*

20. ___ If you receive an error similar to what is displayed in Figure 13–12, then the eClient application configuration and deployment was not successful.


500 Internal Server Error - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
Done
Local intranet

Address http://localhost/eClient81/IDMInit

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, you@your.address and inform them of the time the error occurred, and anything you might have done that may have caused the error.

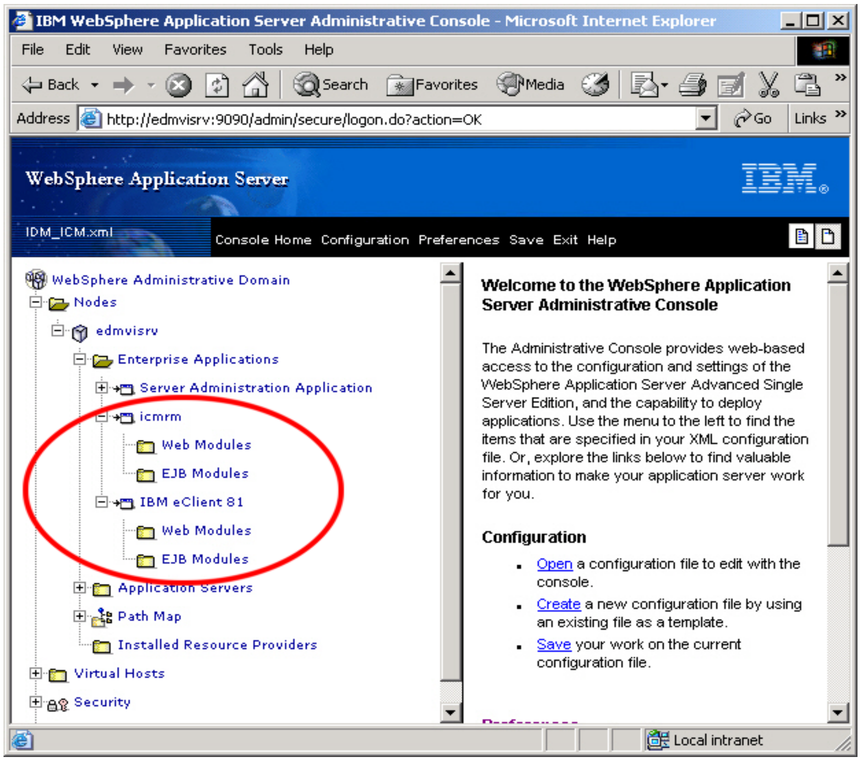
More information about this error may be available in the server error log.

Figure 13–12 *Error initiating the eClient*

21. ___ If the error has been encountered, access WebSphere to check on the eClient and start the eClient application.

   a. Select **Start**.
   b. Select **IBM WebSphere**.
   c. Select **Application Server 4.0 AES**.
   d. Select **Administrator’s Console**.
   e. Type **admin** to logon to the WebSphere Application Server.
   f. Select **Configuration** on the WebSphere Application Server.
   g. Select **Enter full path to file on server**.
   h. Type **C:\Program Files\IBM\Cmgmt\IDM_ICM.xml** for the configuration file name.
   i. Select **OK**.
   j. The **IDM_ICM.xml** file name will be displayed below the WebSphere Application Server screen label to verify the correct XML file is being used.
   k. Select **Nodes**.
   l. Select the **server hostname**.
   m. Select **Enterprise Applications**. Notice the circled areas on Figure 13–13.
   n. Select **IBM eClient 81**.
   o. Select **Start as the Execute State**.
   p. Select **OK**.
   q. After the list of applications has been displayed, select the I**BM eClient 81** check box.
   r. Select **Start**.
   s. Select **Save** to save the configuration file update.
   t. Type **http://localhost/eClient81/IDMInit** on an Internet Explorer window to invoke the eClient.

   If you encounter problems starting the eClient, refer to the troubleshooting section of this guide.


IBM WebSphere Application Server Administrative Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://edmvisrv:9090/admin/secure/logon.do?action=OK
Go Links
WebSphere Application Server
IBM
IDM_ICM.xml
Console Home Configuration Preferences Save Exit Help
WebSphere Administrative Domain
Nodes
edmvisrv
Enterprise Applications
Server Administration Application
icmrm
Web Modules
EJB Modules
IBM eClient 81
Web Modules
EJB Modules
Application Servers
Path Map
Installed Resource Providers
Virtual Hosts
Security
Local intranet

Welcome to the WebSphere Application Server Administrative Console

The Administrative Console provides web-based access to the configuration and settings of the WebSphere Application Server Advanced Single Server Edition, and the capability to deploy applications. Use the menu to the left to find the items that are specified in your XML configuration file. Or, explore the links below to find valuable information to make your application server work for you.

Configuration

- Open a configuration file to edit with the console.
- Create a new configuration file by using an existing file as a template.
- Save your work on the current configuration file.

Figure 13–13 *WebSphere Application Server AEs Administrative Console*

22. ___ Logon to the eClient using **icmadmin** and **password**.

23. ___ Make sure you select the **ICMNLSDB (CM8)** server. The first item listed in the server list may be **ICMNLSDB (FED)** for the EIP federated database.

24. ___ Select **Logon**.

25. ___ You should see an eClient screen similar to Figure 13–14 with a single search option. This is how the eClient ships as a default. The next section will demonstrate how to change the eClient properties file to enable the different features supported in the eClient.

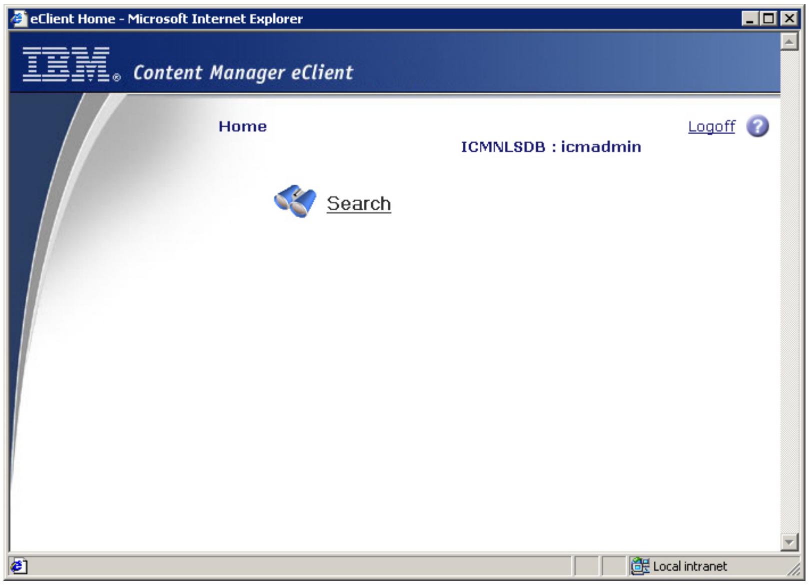
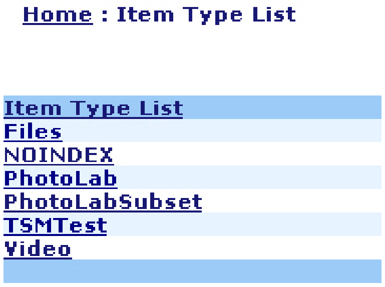


Figure 13–14 *eClient default screen without customized properties.*

26. ___ Select **Search** to verify that the eClient is working against the Content Manager server.

27. ___ The search result list should return a list of item types defined for Content Manager. Notice the PhotoLab and PhotoLabSubset item types in Figure 13–15.

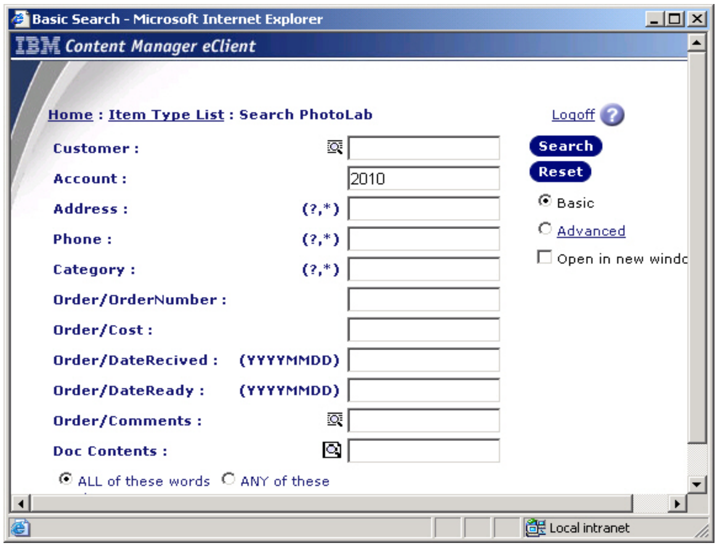


Home : Item Type List

Item Type List
Files
NOINDEX
PhotoLab
PhotoLabSubset
TSMTest
Video

Figure 13–15 *EClient search list listing Content Manager item types*

28. ___ Select the **PhotoLab** item type to display the PhotoLab attributes shown in Figure 13–16.



Basic Search - Microsoft Internet Explorer

IBM Content Manager eClient

Home : Item Type List : Search PhotoLab

Customer :		
Account :		2010
Address :	(?,*)	
Phone :	(?,*)	
Category :	(?,*)	
Order/OrderNumber :		
Order/Cost :		
Order/DateRecived :	(YYYYMMDD)	
Order/DateReady :	(YYYYMMDD)	
Order/Comments :		
Doc Contents :		

● ALL of these words ○ ANY of these

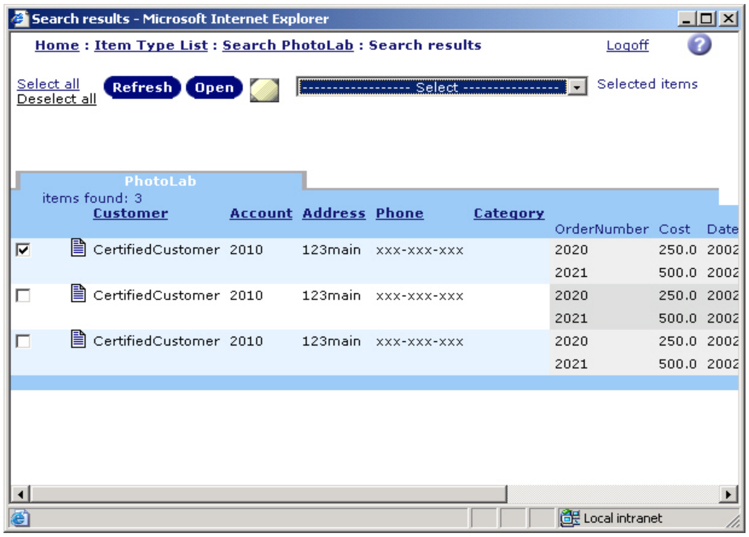
● Basic

○ Advanced

□ Open in new windc

Figure 13–16 *eClient displayed item type attributes for basic search*

29. ___ Type **2010** in the **account attribute field** and select **Search**.



Search results - Microsoft Internet Explorer

Home : Item Type List : Search PhotoLab : Search results

PhotoLab

items found: 3

	Customer	Account	Address	Phone	Category	OrderNumber	Cost	Date
☑	CertifiedCustomer	2010	123main	xxx-xxx-xxx		2020	250.0	2002
						2021	500.0	2002
□	CertifiedCustomer	2010	123main	xxx-xxx-xxx		2020	250.0	2002
						2021	500.0	2002
□	CertifiedCustomer	2010	123main	xxx-xxx-xxx		2020	250.0	2002
						2021	500.0	2002

Figure 13–17 *eClient search results list*

30. ___ If the Client for Windows section of this guide has been completed, the search should return a list of items that have already been imported. The search results list should resemble Figure 13–17.

31. ___ Select one of the items listed in the search results.

32. ___ Select **Open**.

33. ___ The document viewer window will be shown displaying an image similar to Figure 13–18.

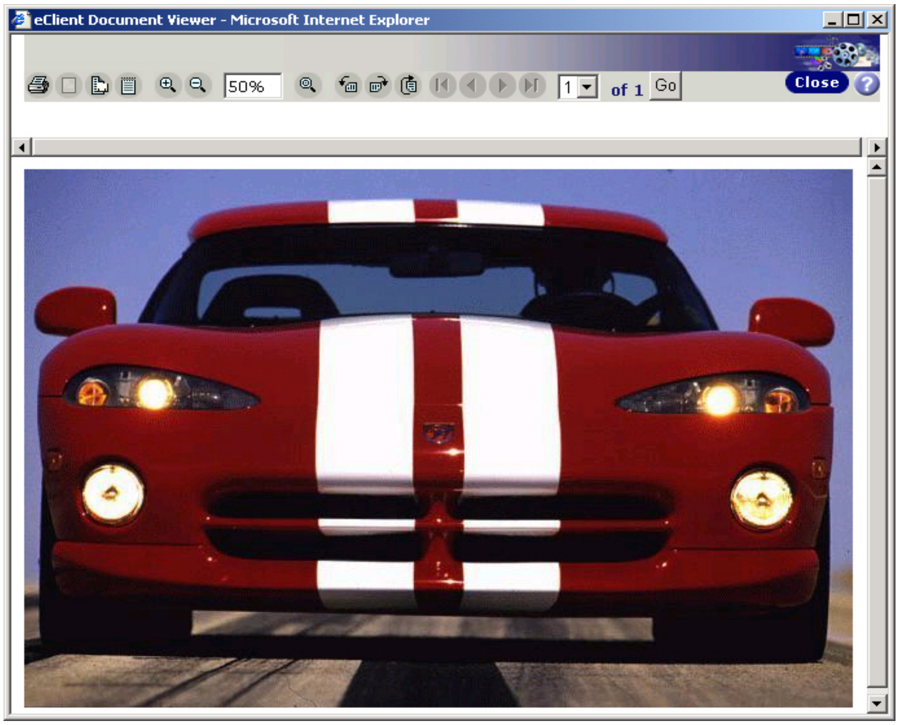


Figure 13–18 *eClient document viewer window*

The above document viewer is dependent on the services of the server to render and display the image. Each time an action is taken it requires the server to update the image. In a later section, the new Viewer Applet will be shown. This ends the eClient installation section of this chapter. The next sections will configure the eClient to import files and work with document routing.

Modify the eClient Property Files

The eClient *IDM.properties* file needs to be modified in order to enable additional features in the eClient. The settings in this file control eClient features such as allowing users to import files, check files in/out, access workflow, email items, and import larger files than the eClient default. There are also settings for setting the eClient trace level, working directories, and connection type. Settings in this section also affect display characteristics for the eClient. A sample of the tag settings from this file have been included in Table 13–2 on page 422. The default location of the *IDM.properties* is the \CMeClient directory. To modify the settings in this file, use an ASCII based editor like the Windows Notepad. There is no graphical interface utility to make desired changes. Changes made in the file will take affect the next time the eClient property daemon checks the properties. If you have disabled the property daemon, you must restart the eClient web application to make the changes effective.

Along with the *IDM.properties*, the *IDMadminDefaults.properties* file controls the default display actions for objects retrieved from Content Manager. For each of the supported MIME types that can be viewed you can specify ***launch*** to launch the viewer, ***applet*** to use the new eClient applet viewer, or ***don't launch*** to force a file conversion on the server to a rendered type that can be handled by the browser. The *IDMadminDefaults.properties* file also controls the file extensions assigned to objects retrieved from the system. The following are sample entries from the *IDMadminDefaults.properties* file.

```
application/pdf=launch
application/vnd.ibm.modcap=don't launch
image/gif=applet
image/jpeg=applet
image/tiff=don't launch
text/html=launch

application/pdf.extension=pdf
application/vnd.ibm.modcap.extension=mda
image/gif.extension=gif
image/jpeg.extension=jpg
image/tiff.extension=tif
text/html.extension=htm
```

Table 13–2 *eClient IDM.properties configuration file example values*

Property Tag	Setting Purpose
TraceLevel	0 = tracing off. 1 = exceptions and errors. 2 = level 1 general info, method entry/exit points. 3 = level 2 with API calls. 4 = level 3 with EIP non-visual bean tracing. 5 = performance tracing.
WorkingDir	Logging, tracing, and data conversion directory.
CacheDir	Storage area for document caching.
ImageURL	Path for the jsp images.
MaxResults	Maximum search results displayed per screen. Default is 10.
TotalMaxResults	Maximum search results retrieved from the server per search criteria. Default is -1 for all hits.
cmbCC2MimeURL	Location of the cmbcc2mime.ini file consisting of the content classes associated with a MIME type.
CsIniURL	Location of the cmbcs.ini configuration file for the EIP connectors.
ICMServersURL	Location of the CMV8 server initialization file.
ConnectionType	0 = local, 1 = remote, 2 = dynamic.
max_import_file_size	Maximum file size allowed during import. Default is 2mb.
workFlowEnabled	Enable/Disable the workflow functionality. Default is false.
checkInOutEnabled	Enable/Disable check in/out capabilities. Default is false.
reIndexEnabled	Enable/Disable reindexing of documents. Default is false.
viewerAppletEnabled	Enable/Disable Applet Viewer. Default is false.
importSupported	Enable/Disable import. Default is false.
CreateFolderEnabled	Enable/Disable create folders. Default is false.
emailEnabled	Enable/Disable email support. Default is false.

Table 13–2 *eClient IDM.properties configuration file example values*

Property Tag	Setting Purpose
directRetrieveEnabled	Enable/Disable direct retrieve from V8 Resource Manager. Default = True.

Modify the IDM.properties File

1. ___ Open the **C:\Program Files\CmeClient\IDM.properties** file in Notepad.
2. ___ Use Table 13–3 to modify the indicated settings.
3. ___ Use care in modifying the settings to avoid altering the comment lines and tags that do not need to be changed at this time.
4. ___ Make sure that the entry **viewerAppletEnabled=true** is set so the applet viewer can be used later in this section. The *Viewer Applet* provides support for client based image rotation, zooming, thumbnails and annotations.

> **Note:** In order for the Viewer Applet to be used **viewerAppletEnabled** must be set to **true** and the MIME type for the file must be set to **applet** in the *IDMadminDefaults.properties* file.

Table 13–3 *Values for modifying the IDM.properties*

Field	Value
workFlowEnabled	True
reIndexEnabled	True
viewerAppletEnabled	True
importSupported	True
CreateFolderEnabled	True
max_import_file_size	200000000
checkInOutEnabled	True

5. ___ Save and Close IDM.properties.

Modify the IDMadminDefaults.properties

1. ___ Open the **C:\CmeClient\IDMadminDefaults.properties** file in Notepad.
2. ___ Change *image/jpeg=don't launch* to **image/jpeg=applet**.
3. ___ Change *text/plain=don't launch* to **text/plain=applet**.
4. ___ Change *image/tiff=don't launch* to **image/tiff=applet**.
5. ___ **Save** and **Close** the IDMadminDefaults.properties file.

Import Using eClient

Now that the Content Manager eClient property files have been modified, the initial eClient application screen should now display Search, Worklists, Import and Create Folder. Your eClient screen should resemble Figure 13-19. This section will cover the importing of files, a new feature in the Content Manager eClient version 8.1.

1. ___ Open an **Internet Explorer** window.
2. ___ Type **http://localhost/eClient81/IDMInit** as the URL, press **Enter**.
3. ___ On the logon page, select **icmnlsdb (CM8)** as Server.
4. ___ Logon using **icmadmin** and **password**.

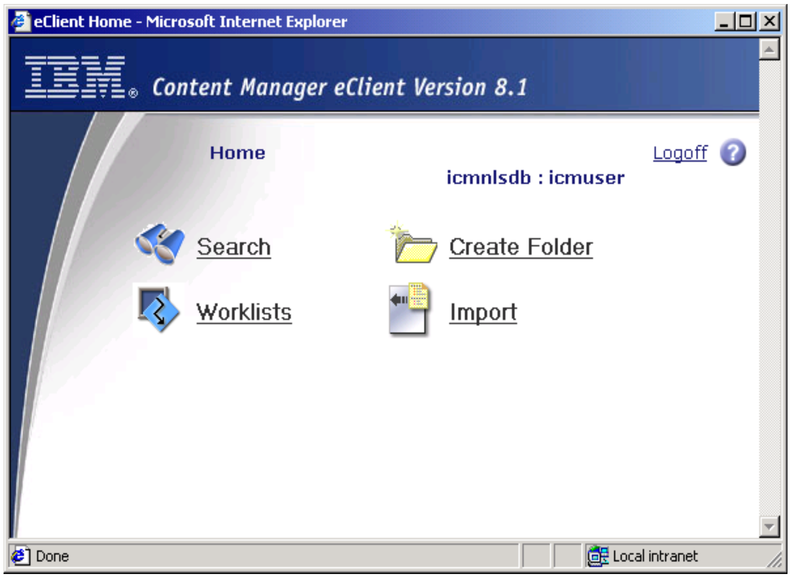


Figure 13-19 *eClient home page after enabling options in IDM.properties*

5. ___ Select **Import**.
6. ___ Select the **PhotoLab** item type.
7. ___ Use Table 13–4 and Table 13–5 on page 426 to complete the attributes for the PhotoLab item type.

Table 13–4 *Attribute values used for importing a PhotoLab item*

Attribute	Value
Customer	Mary
Account	2002
Address	123 Main Street
Phone	972-280-0000

Table 13–5 *Attribute values for order child component*

Order Number	Costs	Date Received	Date Ready	Comments
1001	200.00	2002-10-31	2002-11-15	Family Photos
1002	100.00	2002-10-31	2002-11-12	Car photos

8. ___ Notice the **Order** child level component.

9. ___ Select the **plus sign (+)** to add the second row of child level attributes.

10. ___ Select **Image/Jpeg** as the file type.

11. ___ Select **Typical image document** as the content type.

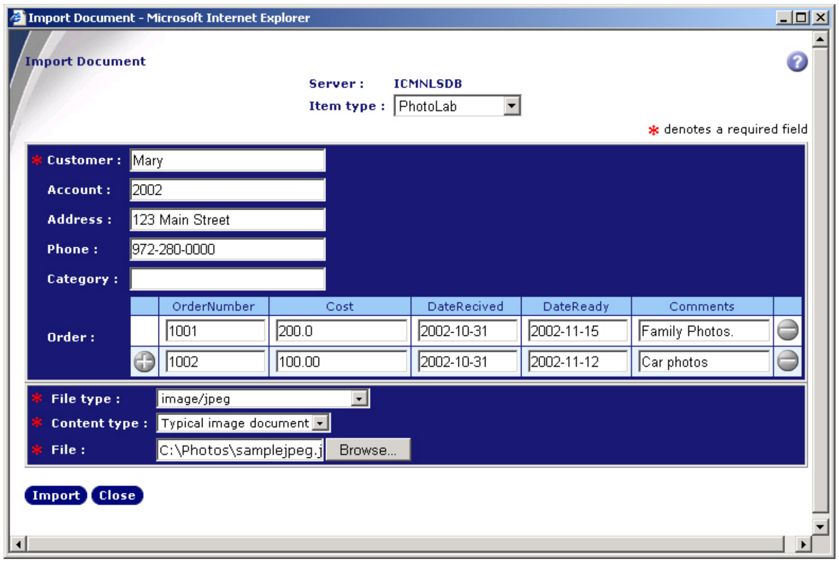
12. ___ Select a JPEG image file to import.

13. ___ The import screen should resemble Figure 13–20.

14. ___ Select **Import**.

15. ___ After the import is done, the Imported Document confirmation screen shown in Figure 13–21 on page 427 should be displayed.

16. ___ Select **Close** to close the document import confirmation window.



Import Document

Server : ICMNLSDB
Item type : PhotoLab

* denotes a required field

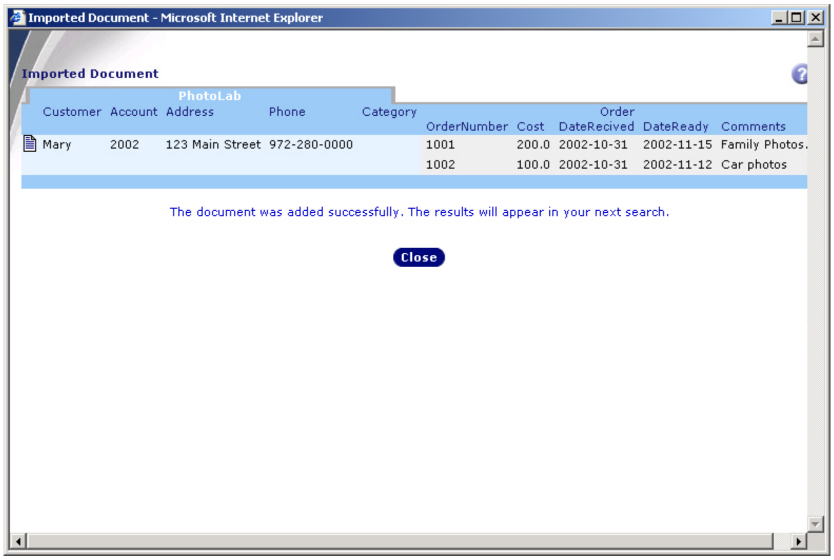
* Customer : Mary
Account : 2002
Address : 123 Main Street
Phone : 972-280-0000
Category :

Order :

OrderNumber	Cost	DateRecived	DateReady	Comments
1001	200.0	2002-10-31	2002-11-15	Family Photos.
1002	100.00	2002-10-31	2002-11-12	Car photos

* File type : image/jpeg
* Content type : Typical image document
* File : C:\Photos\samplejpeg.j

Figure 13–20 *eClient import screen using PhotoLab sample item type*



Imported Document

PhotoLab

Customer	Account	Address	Phone	Category	Order				
					OrderNumber	Cost	DateRecived	DateReady	Comments
Mary	2002	123 Main Street	972-280-0000		1001	200.0	2002-10-31	2002-11-15	Family Photos.
					1002	100.0	2002-10-31	2002-11-12	Car photos

The document was added successfully. The results will appear in your next search.

Figure 13–21 *eClient document import confirmation window*

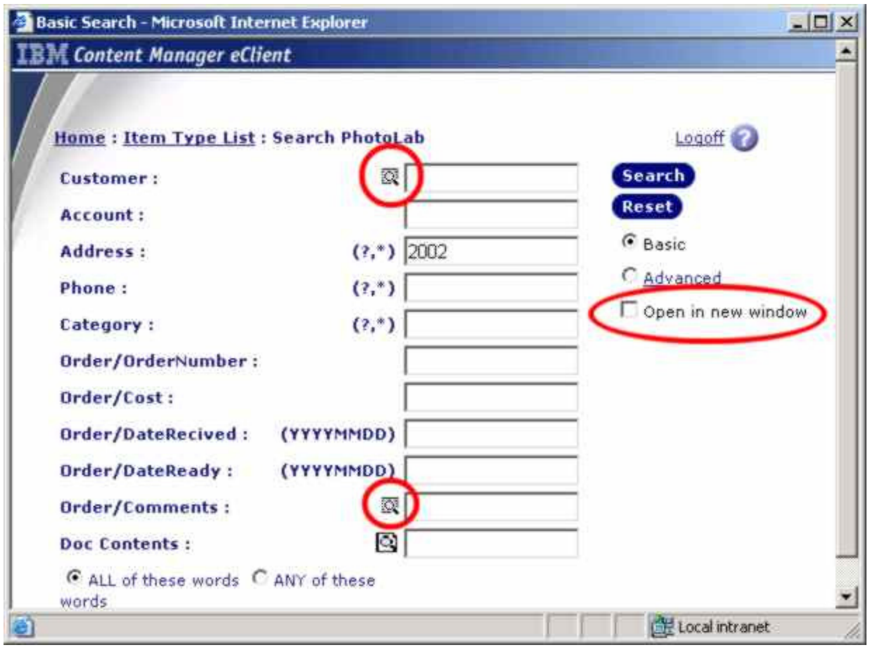
Searching for Imported Images

With photos imported into the system, use the Content Manager eClient for basic search to search for photos. This section will show how the eClient presents the child level attributes for query.

1. ___ Select **Search** for a screen similar to Figure 13–22.
2. ___ Select **PhotoLab** as the item type.

   Basic is selected as the default search for the eClient.

3. ___ Type **2002** as the value for the **Account**.



Basic Search - Microsoft Internet Explorer
IBM Content Manager eClient
Home : Item Type List : Search PhotoLab
Logoff
Search
Reset
Local intranet

Customer :		
Account :		
Address :	(?,*)	2002
Phone :	(?,*)	
Category :	(?,*)	
Order/OrderNumber :		
Order/Cost :		
Order/DateRecived :	(YYYYMMDD)	
Order/DateReady :	(YYYYMMDD)	
Order/Comments :		
Doc Contents :		

● ALL of these words ○ ANY of these words

● Basic
○ Advanced
□ Open in new window

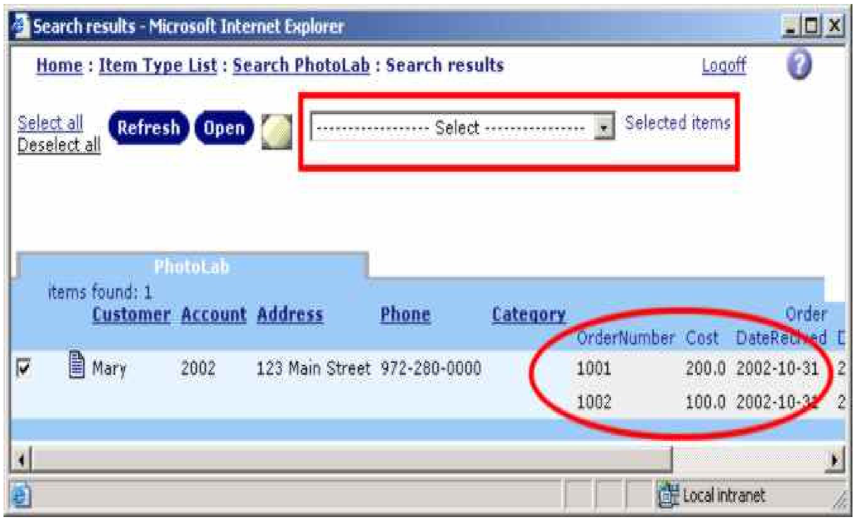
Figure 13–22 *eClient basic search facility*

4. ___ In Figure 13–22 notice the magnifying glass next to the customer and order/comments attribute fields. This indicates that those fields have been setup in the item type for text search indexing.
5. ___ In Figure 13–22 notice the circle around *Open in new window*. When selected the search results will be returned in a new browser window.

8.1 **Note:** When the PhotoLab item type was setup, text search was selected on the item type definition screen, on the Document Management part assignment screen, and could also have been selected for each of the attributes. Strings entered on the ***Doc Content*** line searches the contents of the loaded documents.

6. ___ In Figure 13–22 notice **Order** proceeding some of the attributes. These are the item type child level attributes used to allow multi-valued attributes. The multi-value attributes are shown in the search results list in Figure 13–23.

7. ___ Select **Search**.


Search results - Microsoft Internet Explorer
Home : Item Type List : Search PhotoLab : Search results
Logoff
Select all
Deselect all
Refresh
Open
------------------ Select ----------------
Selected items
PhotoLab
Local intranet

items found: 1

		Customer	Account	Address	Phone	Category	Order OrderNumber	Cost	DateReceived	D
☑		Mary	2002	123 Main Street	972-280-0000		1001	200.0	2002-10-31	2
							1002	100.0	2002-10-31	2

Figure 13–23 *eClient search results window*

8. ___ On the search results screen Figure 13–23, notice how the child level attributes are listed (circled area). When the images were saved, two values were entered for each of the attributes listed under the child component **Order**.

9. ___ Notice the **Selected Items** drop down list box in the rectangle highlight box. When expanded the action items shown in Figure 13–24 on page 430 are listed.

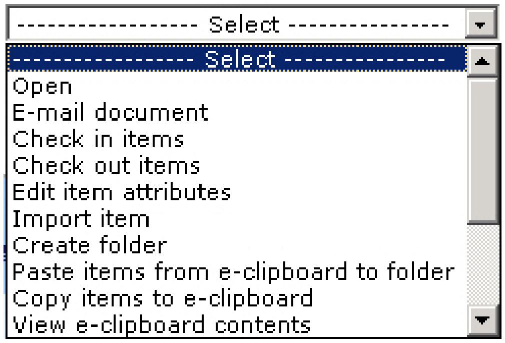
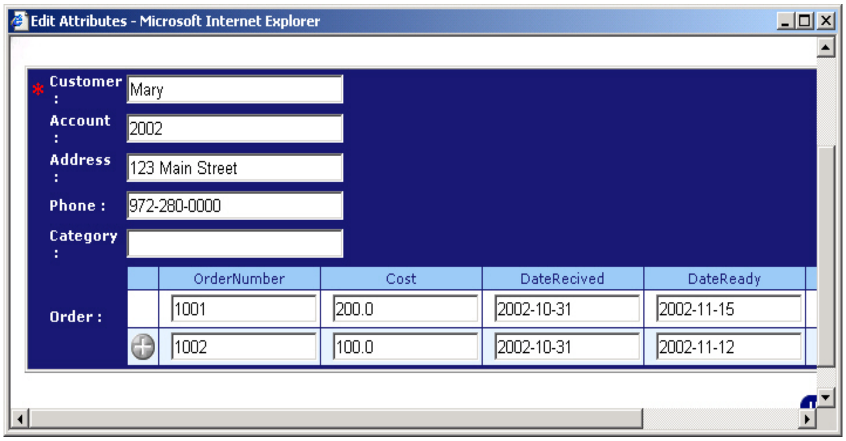

------------------ Select ----------------
------------------ Select ----------------
Open
E-mail document
Check in items
Check out items
Edit item attributes
Import item
Create folder
Paste items from e-clipboard to folder
Copy items to e-clipboard
View e-clipboard contents

Figure 13–24 *eClient basic search results action list*

10. ___ Select **Edit item attributes** from the search results action list to display a screen similar to Figure 13–25.



* Customer : Mary

Account : 2002

Address : 123 Main Street

Phone : 972-280-0000

Category :

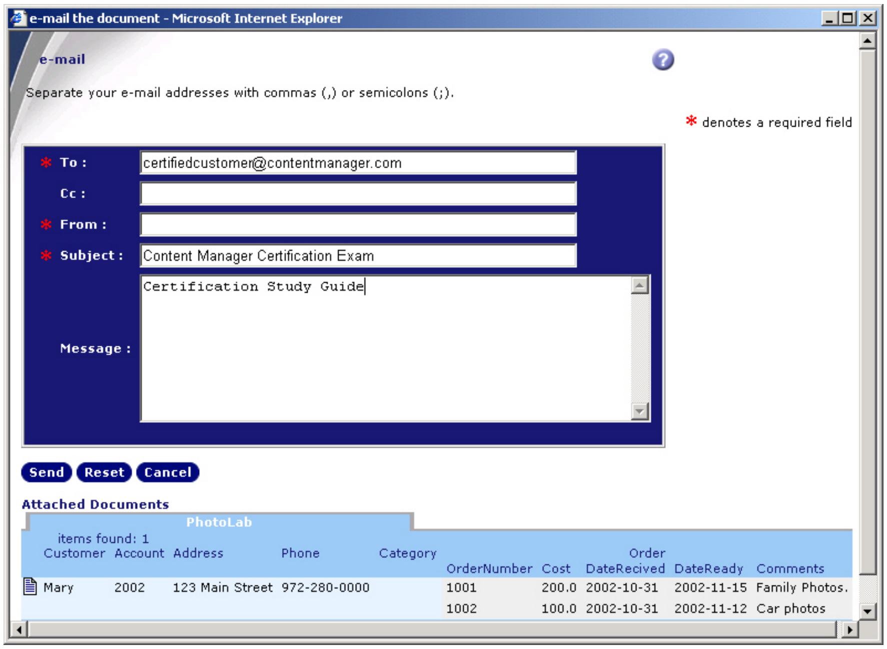
Order :

	OrderNumber	Cost	DateRecived	DateReady
	1001	200.0	2002-10-31	2002-11-15
⊕	1002	100.0	2002-10-31	2002-11-12

Figure 13–25 *eClient item attributes screen*

11. ___ Close the eClient attributes window.

12. ___ Select **Email document** from the search results action list to display a screen similar to Figure 13–26 on page 431. Notice the selected item is listed as an attachment.



e-mail

Separate your e-mail addresses with commas (,) or semicolons (;).

* denotes a required field

* To : certifiedcustomer@contentmanager.com

Cc :

* From :

* Subject : Content Manager Certification Exam

Message : Certification Study Guide

Attached Documents

PhotoLab

items found: 1

Customer	Account	Address	Phone	Category	Order OrderNumber	Cost	DateRecived	DateReady	Comments
Mary	2002	123 Main Street	972-280-0000		1001	200.0	2002-10-31	2002-11-15	Family Photos.
					1002	100.0	2002-10-31	2002-11-12	Car photos

Figure 13–26 *eClient email support for mailing items from a hit list*

13. ___ Select **Cancel** on the email window.

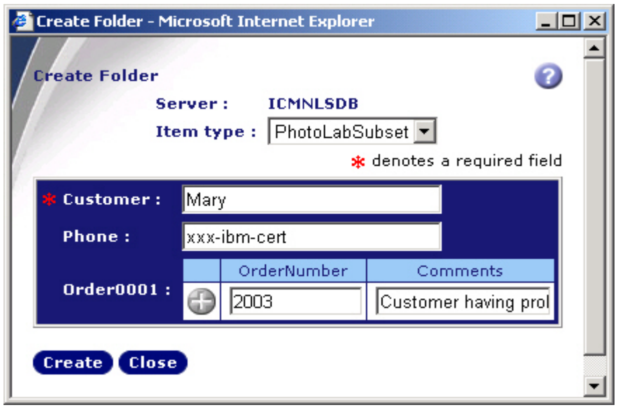
14. ___ Select **Create Folder** from the search results action list.

15. ___ Select **PhotoLabSubset** as the item type. You should see a screen similar to Figure 13–27 on page 432.

16. ___ Use Table 13–6 to complete the folder attributes.

Table 13–6 *Attribute values to create folder entry*

Attribute Field	Attribute Value
Customer	Mary
Phone	xxx-ibm-cert
Order001	2003
Comments	Customer having problems with order.



Create Folder - Microsoft Internet Explorer

Create Folder

Server : ICMNLSDB

Item type : PhotoLabSubset

* denotes a required field

* Customer : Mary

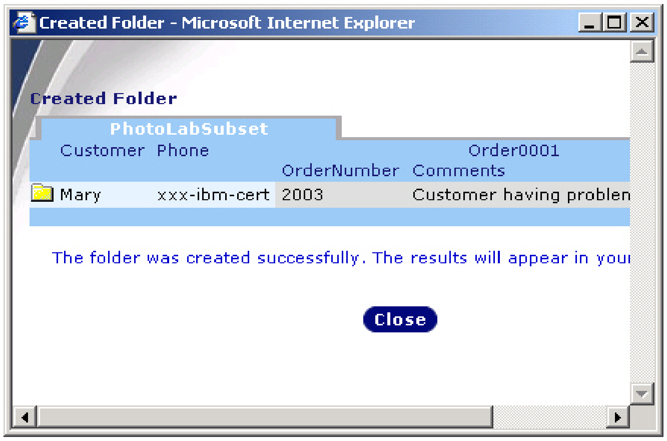
Phone : xxx-ibm-cert

Order0001 :

OrderNumber	Comments
2003	Customer having prol

Figure 13–27 *eClient create folder screen*

17. ___ Select **Create** to finish creating the folder. You should receive a confirmation screen (see Figure 13–28) indicating the folder has been created.



Created Folder - Microsoft Internet Explorer

Created Folder

PhotoLabSubset

Customer	Phone	Order0001 OrderNumber	Comments
Mary	xxx-ibm-cert	2003	Customer having problen

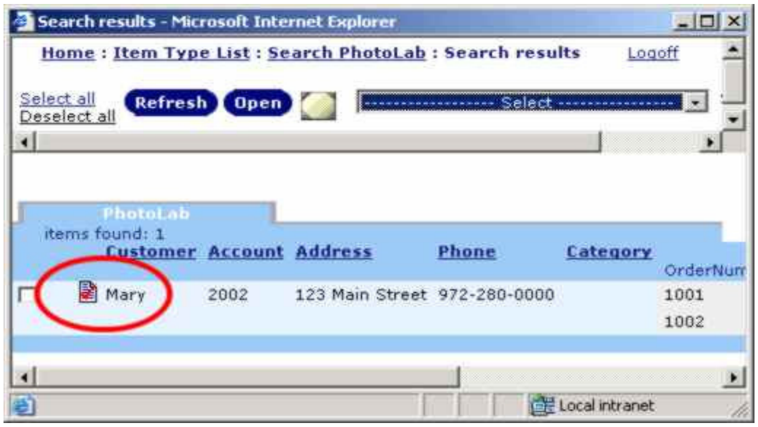
The folder was created successfully. The results will appear in youi

Figure 13–28 *Create folder confirmation screen*

18. ___ Select **Close** on the *folder confirmation* screen.

19. ___ Back on the **Search results** screen, make sure that an item has been select.

20. ___ From the *Selected items list*, select **Check out items**.


Search results - Microsoft Internet Explorer
Home : Item Type List : Search PhotoLab : Search results
Logoff
Select all
Deselect all
Refresh
Open
------------------- Select -----------------
PhotoLab
Local intranet

items found: 1

	Customer	Account	Address	Phone	Category	OrderNum
□	Mary	2002	123 Main Street	972-280-0000		1001 1002

Figure 13–29 *eClient checked out item in results list*

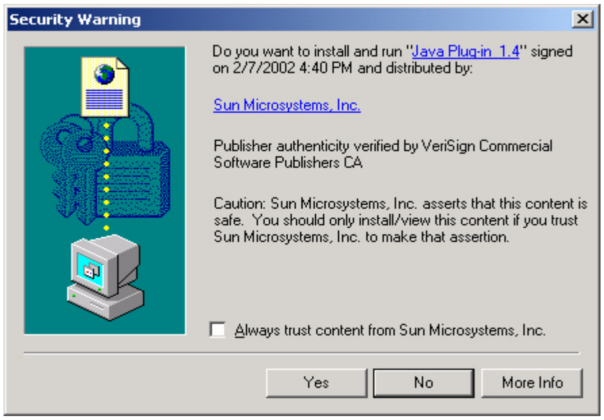
21. ___ Notice in Figure 13–29 that the icon representing the item has been updated with a red check mark.

22. ___ Now for the checked out item, from the *Selected items list*, select **Open.**

23. ___ Remember that in *IDMadminDefaults.properties* file the setting for JPEG images was modified to display the Viewer Applet; **image/jpeg=applet.** Because of this, the Viewer Applet will be called to display and handle the image.

24. ___ If this is the first time the Viewer Applet has been invoked, you will see a screen similar to Figure 13–30 on page 434 indicating that a Java plug-in needs to be installed. Select **Yes** to the options for setting up the plug-in. If you encounter an error, you may need to close and restart the browser.

25. ___ From the *Selected items list*, select **Check in items.** To check back in the file checked out earlier.



Do you want to install and run "Java Plug-in 1.4" signed on 2/7/2002 4:40 PM and distributed by:

Sun Microsystems, Inc.

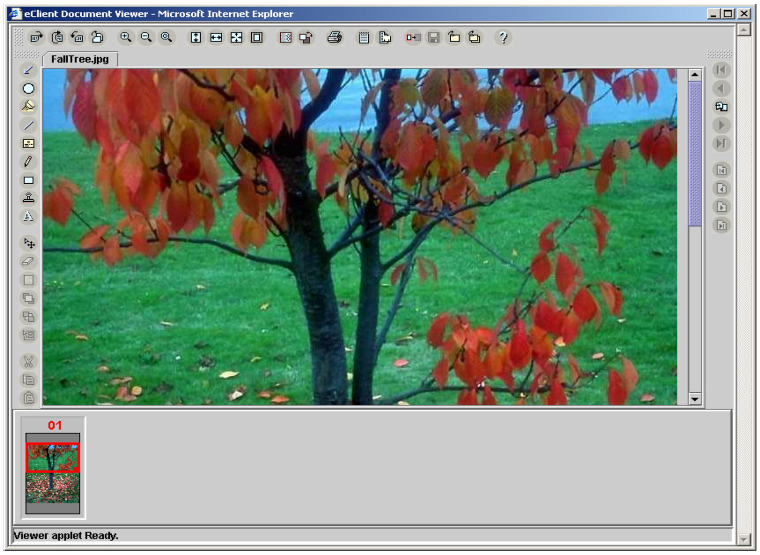
Publisher authenticity verified by VeriSign Commercial Software Publishers CA

Caution: Sun Microsystems, Inc. asserts that this content is safe. You should only install/view this content if you trust Sun Microsystems, Inc. to make that assertion.

□ Always trust content from Sun Microsystems, Inc.

Figure 13–30 *eClient download the required Java plug-in support*

26. ___ Once the Java plug-in has been installed the Viewer Applet should be displayed. An example is provided in Figure 13–31.



Viewer applet Ready.

Figure 13–31 *eClient Viewer Applet*

27. ___ If the Viewer Applet is not displayed and a java exception error is encountered, follow the steps in the Enable eClient Viewer Applet section to copy the required jar files into the eClient WebSphere application directory.

Enable eClient Viewer Applet

If you receive a Java exception error when opening files designated in *IDMadminDefaults.properties* to be handled by the eClient Viewer Applet the following steps may need to be taken to copy the required jar files to the eClient WebSphere application directory. These steps are only required if you plan to retrieve and view files using the ViewerApplet. They are not required if the standard browser viewer is being used.

1. ___ Stop the eClient application by running the following command.

   c:\Program Files\CMeClient\save\stopidmaes.bat

2. ___ Open the **EIP Development Window.**

   Start | Program Files | Enterprise Information Portal | Development Window

3. ___ Make sure there is a \temp directory.

4. ___ Type cd **c:\temp** to switch to the temp directory.

5. ___ Type **jar -xvf c:\Progra~1\CMeClient\eClient81.ear** and press enter.

   This command extracts the eClient81 ear archive into the temporary directory.

6. ___ Type **jar -xvf eClient81.war viewApplet.jar cmbview81.jar** and press enter.

   This command extracts the viewApplet.jar and cmbview81.jar files from the eClient81.war file.

7. ___ Type the following move command to move the Viewer Applet jar file to the eClient WebSphere application directory.

   move viewerApplet.jar c:\websphere\appserver\installedapps\eclient81.ear\eclient81.war

8. ___ Type the following move command to move the eClient viewer java beans interface to the eClient WebSphere application directory.

   move cmbview81.jar c:\websphere\appserver\installedapps\eclient81.ear\eclient81.war

9. ___ Start the eClient application by running the following command.

   c:\Program Files\CMeClient\save\startidmaes.bat

The System should now be ready to handle viewing objects using the Viewer Applet.

Using Text Search

Documents, text files, and other document objects for which Content Manager provides conversions can be imported and identified for text indexing. Once the files are imported, they are processed by the DB2 UDB Text Information Extender to create the indexed values. The values are stored on the server in the directory indicated when the item type was created.

1. ___ Select **Import**.
2. ___ Select **PhotoLab** as the item type.
3. ___ Use Table 13–7 to complete the import attributes.

Table 13–7 *Attributes values used for text search*

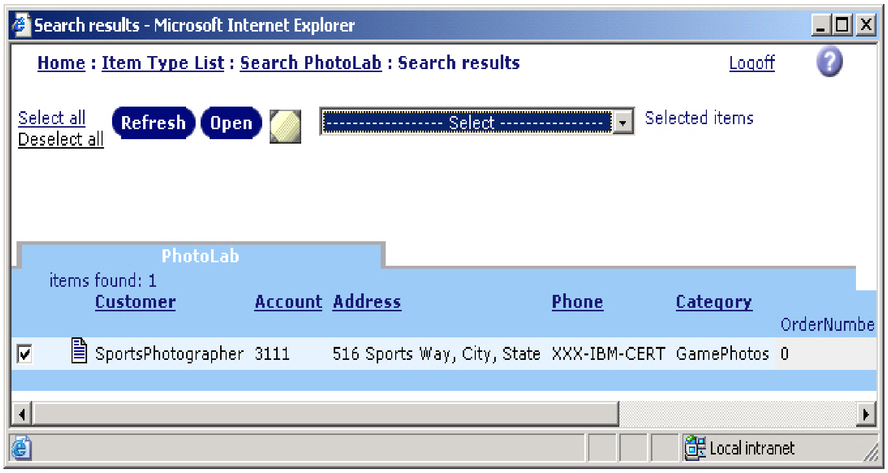
Attribute	Value
*Customer	SportsPhotographer
Account	3111
Address	516 Sports Way, City, State
Phone	XXX-IBM-CERT
Category	GamePhotos

4. ___ Select **Text/plain** as the File Type.
5. ___ Select **Browse** to pick some text files.
6. ___ For now ignore the attributes for the Order child levels.
7. ___ Select **Import**.
8. ___ Select Close to close the imported document confirmation screen.

   Now do a basic search to locate the documents. You may need to give it a few minutes to allow the text search indexing process to complete.

9. ___ Select **Search**.
10. ___ Type a text string that was contained in the imported documents into the **Doc Contents** field.
11. ___ Select **Search**.

    Documents that contain text matching the entered string will be listed in the search results list (see Figure 13–32).


Search results - Microsoft Internet Explorer
Home : Item Type List : Search PhotoLab : Search results
Logoff
Select all
Deselect all
Refresh
Open
----------------- Select ----------------
Selected items
PhotoLab
Local intranet

items found: 1

	Customer	Account	Address	Phone	Category	OrderNumbe
☑	SportsPhotographer	3111	516 Sports Way, City, State	XXX-IBM-CERT	GamePhotos	0

Figure 13–32 *eClient search results from using content text search*

12. ___ Select **Open** from the *Selected items* list.

13. ___ Depending on the settings in the *IDMadminDefaults.properties* file for text documents the browser viewer (**text/plain=don't launch)** or Viewer Applet **(text/plain=applet)** will be displayed.

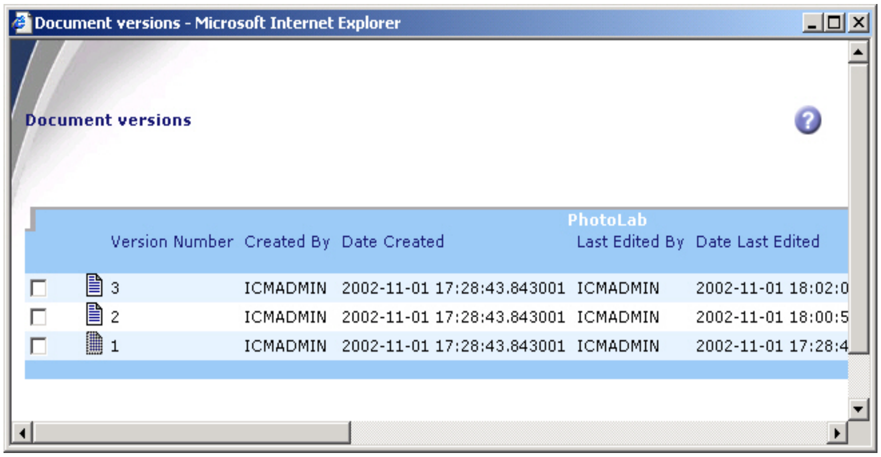
14. ___ For item type attributes that have been setup to be text indexed, contextual searches can be performed using the contains qualifier on the eClient advanced search screen. The difference is when using contains, the search is performed against the text indexed files instead of the Library Server attribute tables. The benefit of this is in cases where you are searching for a document containing a string that might have been also added to an attribute.

Take some time to work with the advanced search to compare the differences between the two search processes.

eClient Version Support

Content Manager Version 8.1 provides support for versioning both the content of imported documents and files, and the attributes defined for those documents and files. As items are modified or annotated using the eClient, a new version is created when the changes have been saved. Dependent on the version count setting for the item type, new versions will be created and once the count has been hit the oldest version is deleted. The following steps will review the version support added to the eClient.

1. ___ Select **Search**.
2. ___ A list of item types is displayed.
3. ___ Select item type **PhotoLab**.
4. ___ Type **2002** as the value for the **Account**.
5. ___ Select **Search**.
6. ___ A list of available items are displayed in the browser.
7. ___ Select an **item**.
8. ___ Open the item and make changes using the highlight annotation tools of the viewer.
9. ___ Save the item changes.
10. ___ Select **View version information** from the *Selected items* drop down list to display the different versions of the document that have been created.
11. ___ From the eClient *Document versions* screen, select a version to display and modify.
12. ___ When saved another version should be created in the version list shown in Figure 13–33.
13. ___ Repeat the step to view versions from the search result list to see the newest version created.



Document versions

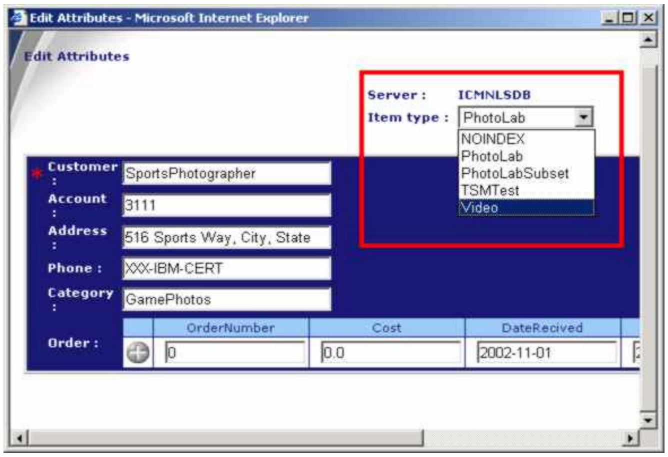
		Version Number	Created By	Date Created	PhotoLab Last Edited By	Date Last Edited
□	🗎	3	ICMADMIN	2002-11-01 17:28:43.843001	ICMADMIN	2002-11-01 18:02:0
□	🗎	2	ICMADMIN	2002-11-01 17:28:43.843001	ICMADMIN	2002-11-01 18:00:5
□	🗎	1	ICMADMIN	2002-11-01 17:28:43.843001	ICMADMIN	2002-11-01 17:28:4

Figure 13–33 *eClient version list*

Re-index Items

Content Manager eClient provides support for re-indexing an item by allowing the item to be reassigned to a different item type. The following steps will walk through the eClient re-index support.

1. ___ Select **Search**.
2. ___ A list of item types is displayed.
3. ___ Select item type **PhotoLab**.
4. ___ Type **2002** as the value for the **Account**.
5. ___ Select **Search**.
6. ___ A list of available items are displayed in the browser.
7. ___ Select an **item**.
8. ___ Select **Edit item attributes** from the *Selected items* drop down list to display the different versions of the document that have been created.



Server : ICMNLSDB

Item type : PhotoLab

* Customer : SportsPhotographer

Account : 3111

Address : 516 Sports Way, City, State

Phone : XXX-IBM-CERT

Category : GamePhotos

Order :

OrderNumber	Cost	DateRecived
0	0.0	2002-11-01

Figure 13-34 *eClient attributes allows changing the item type for the item*

In Figure 13-34 with the item selected and the attributes displayed. The item type drop down list box can be used to switch the item type for the selected item.

Copy Items to a Folder

The Content Manager eClient e-clipboard is primarily used to move documents across folders and other multiple-step processes. This feature is available to all back-end servers.

1. ___ Select **Create Folder** from the eClient screen.

2. ___ Create a folder in the **PhotoLab** item type.

3. ___ Select **Search**.

4. ___ A list of item types is displayed.

5. ___ Select item type **PhotoLab**.

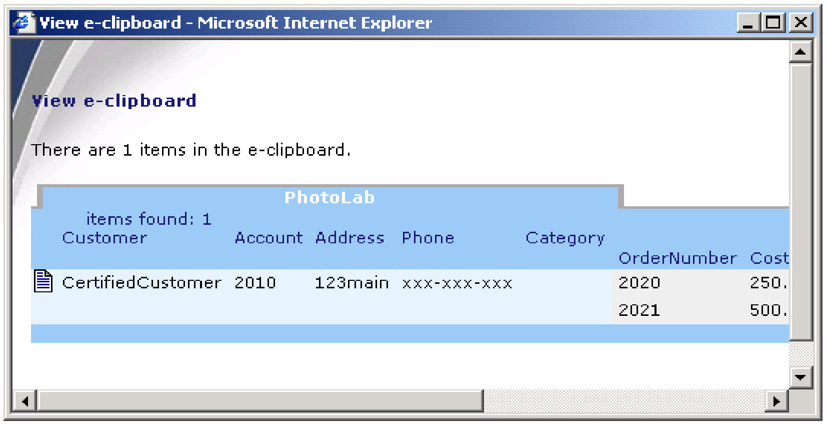
6. ___ Type **2002** as the value for the **Account**.

7. ___ Select **Search**.

8. ___ A list of available items are displayed in the browser.

9. ___ Select an **item**.

10. ___ Select **Copy items to e-clipboard** from the *Selected items* drop down list. The eClient clipboard is shown in Figure 13–35.



View e-clipboard

There are 1 items in the e-clipboard.

PhotoLab

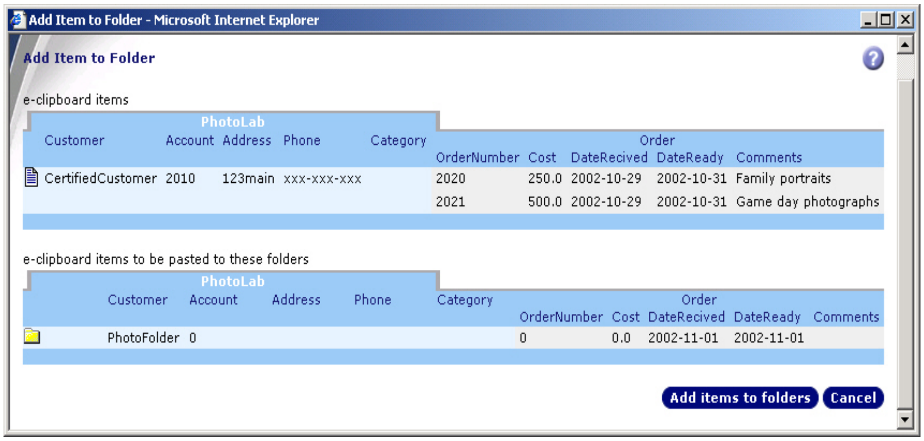
items found: 1

Customer	Account	Address	Phone	Category	OrderNumber	Cost
CertifiedCustomer	2010	123main	xxx-xxx-xxx		2020	250.
					2021	500.

Figure 13–35 *eClient clipboard*

11. ___ Check **the box next to the PhotoFolder** folder.

12. ___ Select **Paste items from e-clipboard to folder** from the drop down list.



Add Item to Folder

e-clipboard items

PhotoLab									
Customer	Account	Address	Phone	Category	Order				
					OrderNumber	Cost	DateRecived	DateReady	Comments
CertifiedCustomer	2010	123main	xxx-xxx-xxx		2020	250.0	2002-10-29	2002-10-31	Family portraits
					2021	500.0	2002-10-29	2002-10-31	Game day photographs

e-clipboard items to be pasted to these folders

PhotoLab									
Customer	Account	Address	Phone	Category	Order				
					OrderNumber	Cost	DateRecived	DateReady	Comments
PhotoFolder	0				0	0.0	2002-11-01	2002-11-01	

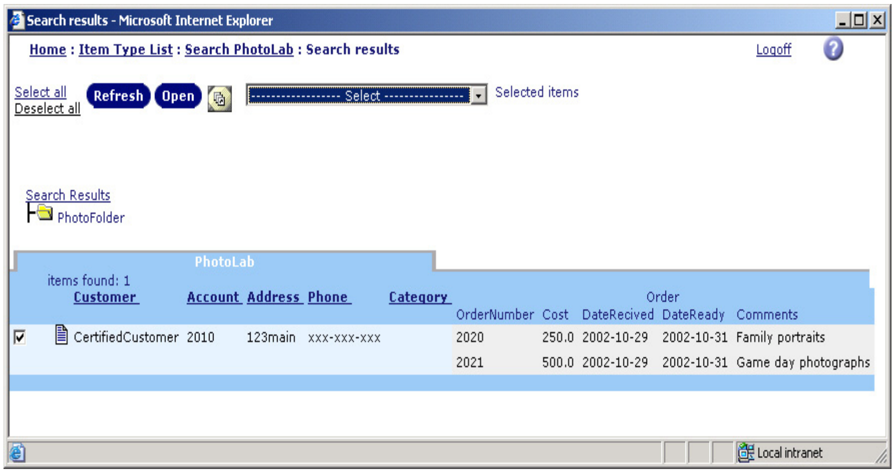
Figure 13-36 *eClient add item to a folder*

13. ___ Select **Add items to folders** (see Figure 13-36).

14. ___ Select **Refresh**.

15. ___ Select **the PhotoFolder** folder.

16. ___ Items in the Photo Folder folder are displayed. (see Figure 13-37)


Search results - Microsoft Internet Explorer
Logoff
Select all
Deselect all
Refresh
Open
------------------ Select ------------------
Selected items
Local intranet

Home : Item Type List : Search PhotoLab : Search results

Search Results
PhotoFolder

items found: 1

PhotoLab										
	Customer	Account	Address	Phone	Category	Order				
						OrderNumber	Cost	DateRecived	DateReady	Comments
☑	CertifiedCustomer	2010	123main	xxx-xxx-xxx		2020	250.0	2002-10-29	2002-10-31	Family portraits
						2021	500.0	2002-10-29	2002-10-31	Game day photographs

Figure 13-37 *eClient document in a folder*

Using Document Routing

The Content Manager eClient provides support for starting documents, images, and other files on a document routing process after they have been imported. Currently there is no way to start items on a process during import. Once objects and folders are started on a document routing process, the eClient user uses the Worklists they can access to work with items residing on the different work nodes. The *select item* action menu provides the document routing actions the user can take on objects and folders represented in the worklist. The available actions are based on how the work node for where the object or folder resides and the process actions defined between the nodes.

1. ___ Select **Search**.

2. ___ A list of item types is displayed.

3. ___ Select item type **PhotoLab**.

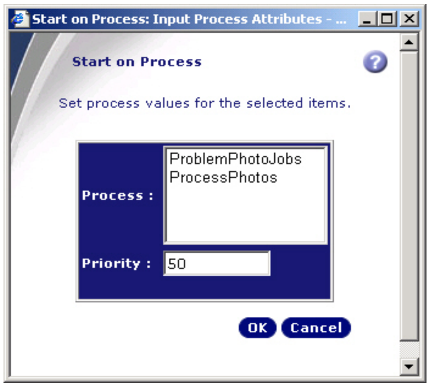
4. ___ Type values into an attribute field.

5. ___ Select **Search**.

6. ___ A list of available items are displayed in the browser.

7. ___ Select a document **item**.

8. ___ Select **Start process** from the *Selected items* drop down list. A screen similar to Figure 13–38 should be displayed.



Start on Process: Input Process Attributes - ...

Start on Process

Set process values for the selected items.

Process : ProblemPhotoJobs, ProcessPhotos

Priority : 50

Figure 13–38 *eClient start document routing process*

9. ___ Select **ProcessPhotos**.

10. ___ Select **OK**.

11. ___ Select **Close** on the start process confirmation screen.

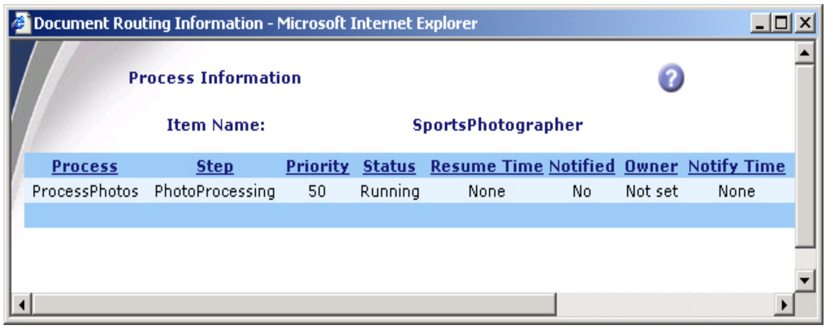
12. ___ Repeat the same action for a folder in the search results hit list.

13. ___ Select **Close** on the *start process confirmation* screen.

14. ___ Go back to the search results list.

15. ___ For the same item that was selected and started on the process, select **Process Information** from the *Selected items* drop down list. This should display a screen similar to Figure 13–39.

16. ___ The same type of information is displayed for folder items on the process.



Document Routing Information - Microsoft Internet Explorer

Process Information

Item Name: SportsPhotographer

Process	Step	Priority	Status	Resume Time	Notified	Owner	Notify Time
ProcessPhotos	PhotoProcessing	50	Running	None	No	Not set	None

Figure 13–39 *eClient item document routing process information*

17. ___ Close the *process information* window.

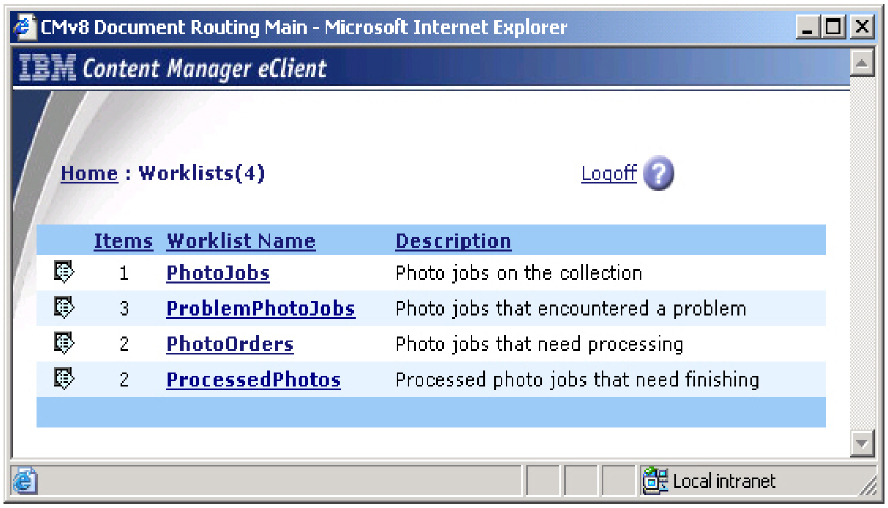
Working Items in a Process

To work with items on a document routing process, the eClient accesses the defined worklist.

1. ___ Select **Worklists**.

2. ___ A list of worklists defined during the document routing section of this guide should be listed. This includes the PhotoJobs, PhotoOrders, ProcessedOrders, and ProblemPhotoJobs worklists, (see Figure 13–40).

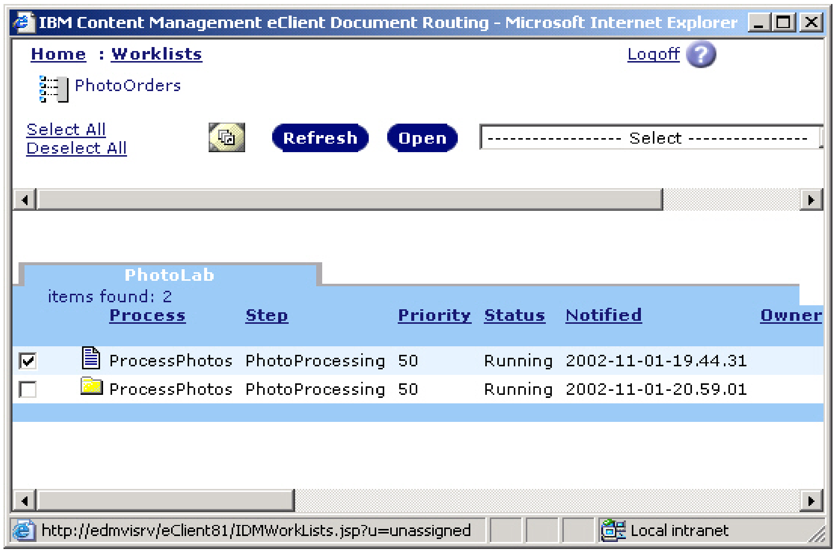
3. ___ Each of the worklists should already have a number of items dependent on the actions taken in earlier sections of this guide, (see Figure 13–41).


CMv8 Document Routing Main - Microsoft Internet Explorer
IBM Content Manager eClient
Home : Worklists(4)
Logoff
Local intranet

	Items	Worklist Name	Description
	1	PhotoJobs	Photo jobs on the collection
	3	ProblemPhotoJobs	Photo jobs that encountered a problem
	2	PhotoOrders	Photo jobs that need processing
	2	ProcessedPhotos	Processed photo jobs that need finishing

Figure 13–40 *eClient document routing Worklists*

4. ___ Open the **PhotoOrder** worklist.


IBM Content Management eClient Document Routing - Microsoft Internet Explorer
Home : Worklists
Logoff
PhotoOrders
Select All
Deselect All
Refresh
Open
----------------- Select ----------------
PhotoLab
items found: 2
http://edmvisrv/eClient81/IDMWorkLists.jsp?u=unassigned
Local intranet

		Process	Step	Priority	Status	Notified	Owner
☑		ProcessPhotos	PhotoProcessing	50	Running	2002-11-01-19.44.31	
□		ProcessPhotos	PhotoProcessing	50	Running	2002-11-01-20.59.01	

Figure 13–41 *Items on a workbasket node represented in a worklist*

5. ___ Select one of the worklist items.

6. ___ Expand ***Selected items*** drop down list to view the actions that apply to document routing. See Figure 13–42 for an example of the document routing actions for a selected item in a worklist.

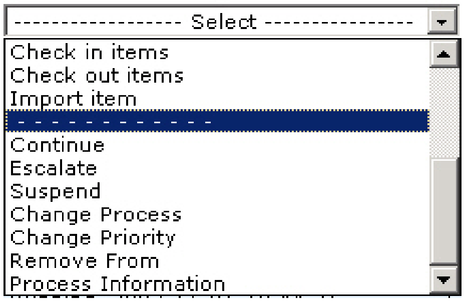


Figure 13–42 *eClient document routing actions for selected item*

7. ___ The document routing available actions will be dependent on the item selected and where the item resides in the process. For example, when the ProcessPhotos process was defined earlier in this guide Continue and Escalate where used as actions to proceed (Continue) to the next node or reroute (Escalate) to a different work node. These are the predefined action labels that come with the system. When the document routing process was setup, other terms could have been used to represent the same process routes. Table 13–8 provides a list of document routing actions that are available for a user to select.

Table 13–8 *eClient document routing process actions*

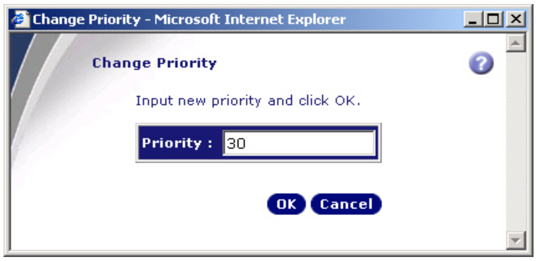
Process Action	Default purpose for the action
Change process	Will display a list of available document routing processes that the selected item can be assigned. This removes the item from the current process.
Continue	One of the predefined acceptable actions defined for this step in the process. In the ProcessPhotos process *continue* moves the item onto the next work node. Any text can be used for an action in the process.

Table 13–8 *eClient document routing process actions*

Process Action	Default purpose for the action
Escalate	One of the predefined acceptable actions defined for this step in the process. In the ProcessPhotos process *escalate* is used re-route the work package referencing the item to a work node other than the normal next step handled by continue. Any text can be used for an action in the process.
Remove from	Delete the item from the process. The item remains in the library system.
Change Priority	Alter the priority for the selected item. The larger the number the lower the priority for the item.
Suspend	Interrupt the process for the item, temporarily suspending the item.
Activate	Reactivate an item that has been suspended.
Process Information.	Display process status information for the selected item.

8. ___ Select one of the items listed in the PhotoOrders worklist and select **Priority** from the **Selected items** drop down list.

Notice the available actions will be different if selecting a document or file started on the process directly versus an item contained in a folder that was started on the process. An item contained in a folder will not have document routing actions in the Selected items listed. This is because when the folder was placed on the process, the folder represents the work package and the files contained in the folder are treated as a single process entity.



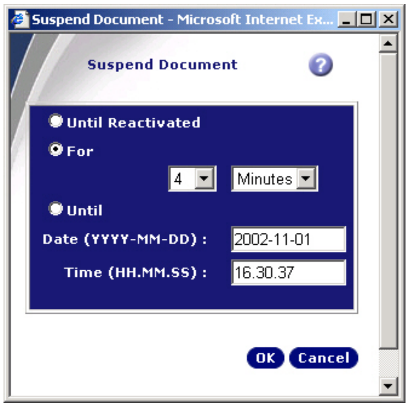
Input new priority and click OK.

Priority : 30

Figure 13–43 *eClient document routing change priority*

9. ___ Change the **Priority** to **30** to give it a higher priority (see Figure 13–43).

10. ___ For the same item now select **Suspend** from the *Selected items* drop down list. Set the **suspend** time to **four minutes** (see Figure 13–44).



Suspend Document - Microsoft Internet Ex...

Suspend Document

○ Until Reactivated

● For

4 Minutes

○ Until

Date (YYYY-MM-DD) : 2002-11-01

Time (HH.MM.SS) : 16.30.37

Figure 13–44 *eClient worklist suspend item*

This will provide an opportunity to see what the client does with items that are reactivated. Notice the suspended item remains in the list of items in the worklist.

11. ___ Select one of the items listed in the PhotoOrders worklist and select **Continue** from the **Selected items** drop down list.

This should have removed the item from the ProcessOrders worklist and moved it to the ProcessedPhotos worklist representing the next work node in the process. ProcessedPhotos should now have an additional item listed.

12. ___ Select one of the items listed in the PhotoOrders worklist and select **Escalate** from the **Selected items** drop down list.

This should have removed the item from the ProcessOrders worklist and moved it to the ProblemPhotoJobs worklist. ProblemPhotoJobs should now have an additional item listed. This was the exception process entered into the ProcessOrders document routing process.

13. ___ Select one of the items listed in the ProcessedPhotos worklist and select **Continue** from the **Selected items** drop down list.

Notice that Escalate is not listed as an action because it was not defined as a valid action for items leaving the Photo Finishing work node. Once items leave the Photo Finishing work node, the next step is the end of the process.

14. ___ Select one of the items listed in the ProblemPhotoJobs worklist and select **Escalate** from the **Selected items** drop down list. This should move the item to the end of the process.

eClient Viewer Applet

The *Viewer Applet* was added to Content Manager eClient 8.1 to provide a better way of performing client side document conversions and for manipulating displayed objects without hitting the server. With the Viewer Applet, the rendering of the image or document is performed at the client application after a direct retrieval of the object from the Resource Manager. As the user performs actions, such as annotating or rotating the displayed object, the resources of the workstation are used to re-render the object with the overlaid annotations. This reduces the performance drain on the eClient application server. If the Viewer Applet is not used, then the Web Viewer will be launched to handle the object requiring the eClient application server to render the object for the viewer. As demonstrated in Figure 13–45, actions taken by users using the browser viewer, such as rotate, will require the eClient application server to re-render the object for the workstation viewer.

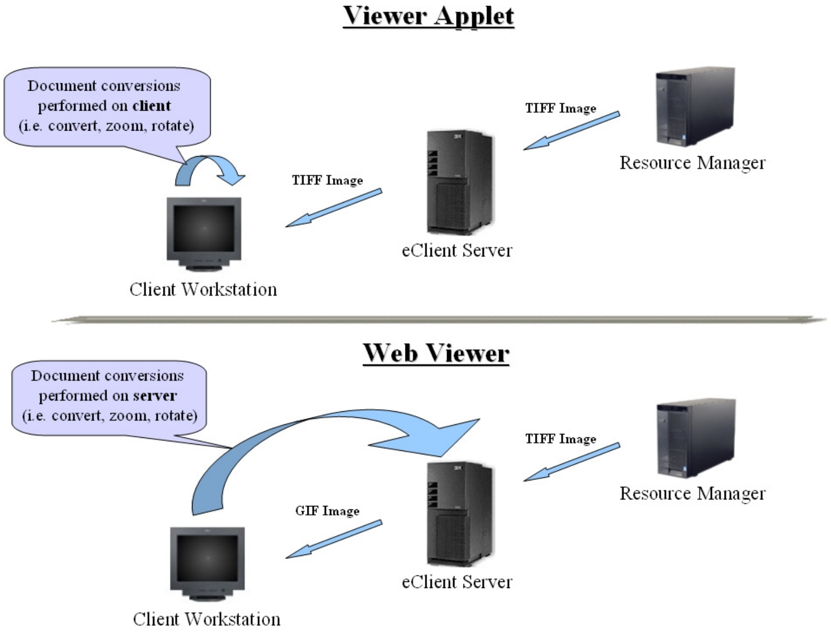


Figure 13–45 *Viewer Applet renders images at the client workstation*

The following steps will demonstrate the Viewer Applet.

1. ___ Select **Search**.
2. ___ A list of item types is displayed.
3. ___ Select item type **PhotoLab**.
4. ___ Type values into an attribute field.
5. ___ Select **Search**.
6. ___ A list of available items are displayed in the browser.
7. ___ Select an **item**.

Based on the prior sections in this chapter it needs to be a JPEG, TIFF, or text file. These were the MIME types set to launch the Viewer applet in the *IDMadminDefaults.properties* file.

8. ___ The content of the file is displayed in the eClient Viewer Applet (see Figure 13-46).

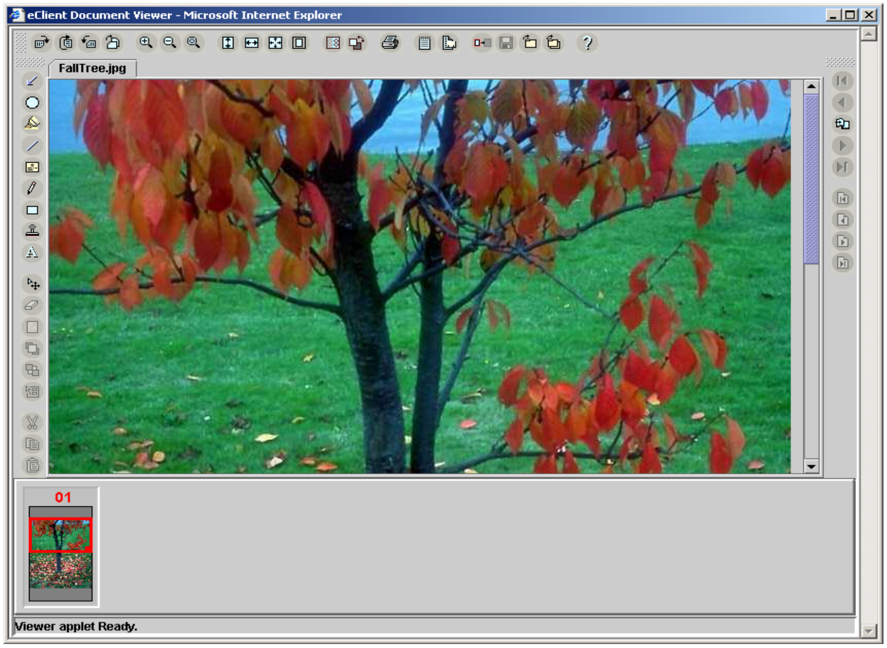


Figure 13-46 *Display document in viewer applet*

9. ___ Select **Zoom In/Out** to view the image in different size.

10. ___ Select **Rotate** to view the image in a different orientation.

11. ___ Select the **Edit/View** the NoteLog icon on the top (seventh icon from right).

12. ___ On left toolbar, select the **Circle** icon and move the cursor into image section.

13. ___ Select and hold on left mouse button and draw a **square**.

14. ___ A circle annotation is made in the photo (see Figure 13-47).

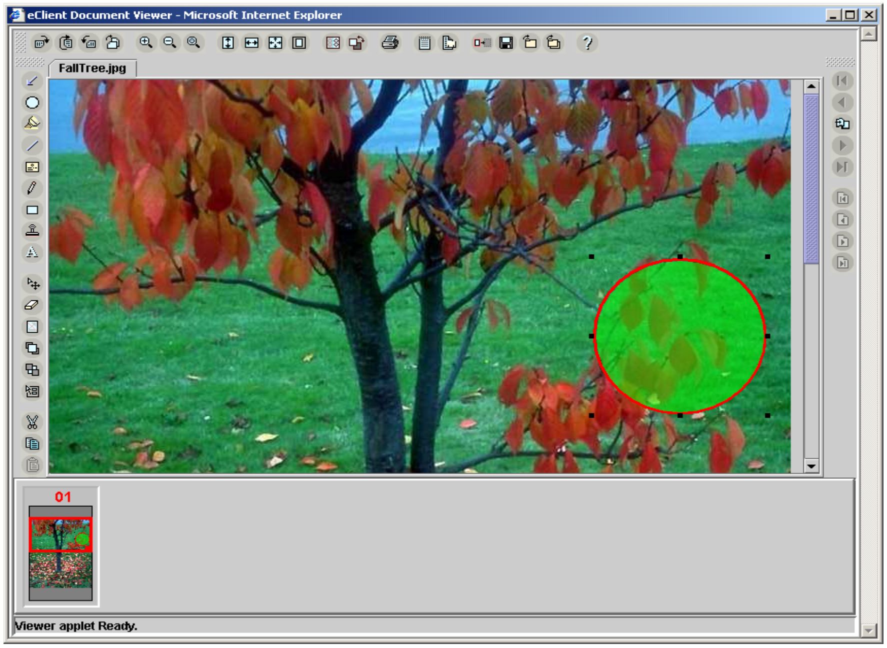


Figure 13-47 *Circle annotation in view applet*

15. ___ On left toolbar, select the **Text** icon and move cursor into image section.

16. ___ Select anywhere in photo area.

17. ___ Enter **This is an annotation test** (see Figure 13-48 on page 452).

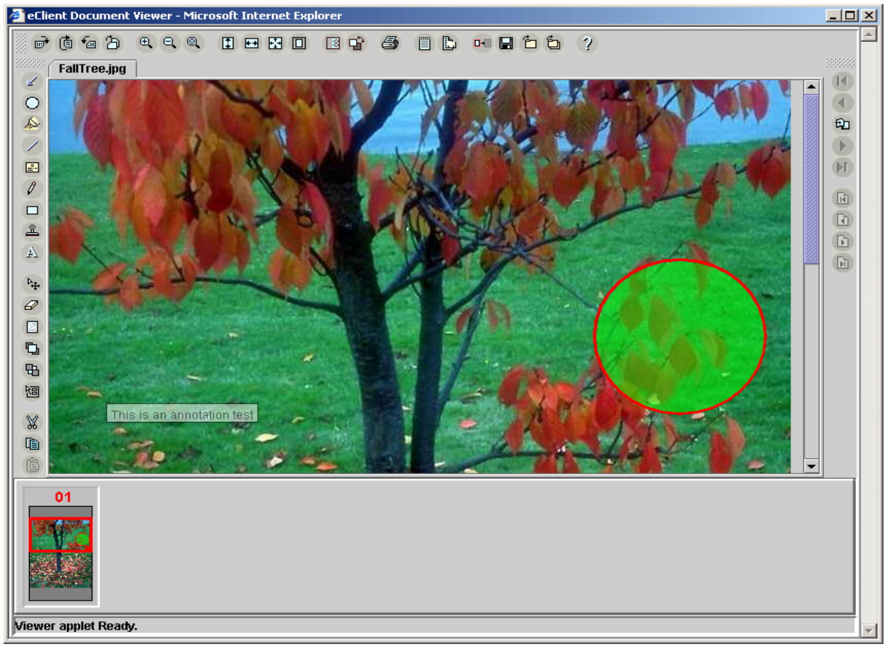

eClient Document Viewer - Microsoft Internet Explorer
FallTree.jpg
This is an annotation test
01
Viewer applet Ready.

Figure 13-48 *Text annotation in viewer applet*

18. ___ On left toolbar, select the **Hide and show annotations** icon (7th icon from the bottom).

19. ___ Both annotations disappear.

20. ___ Select the **Hide and show annotations** icon again annotation re-appears.

21. ___ There are many different types of annotations available.

22. ___ Select **Save Document** icon on the top.

23. ___ Select **Close Document** icon on the top.

24. ___ Re-open the same document or image to display the item in the applet viewer with the annotations.

Summary

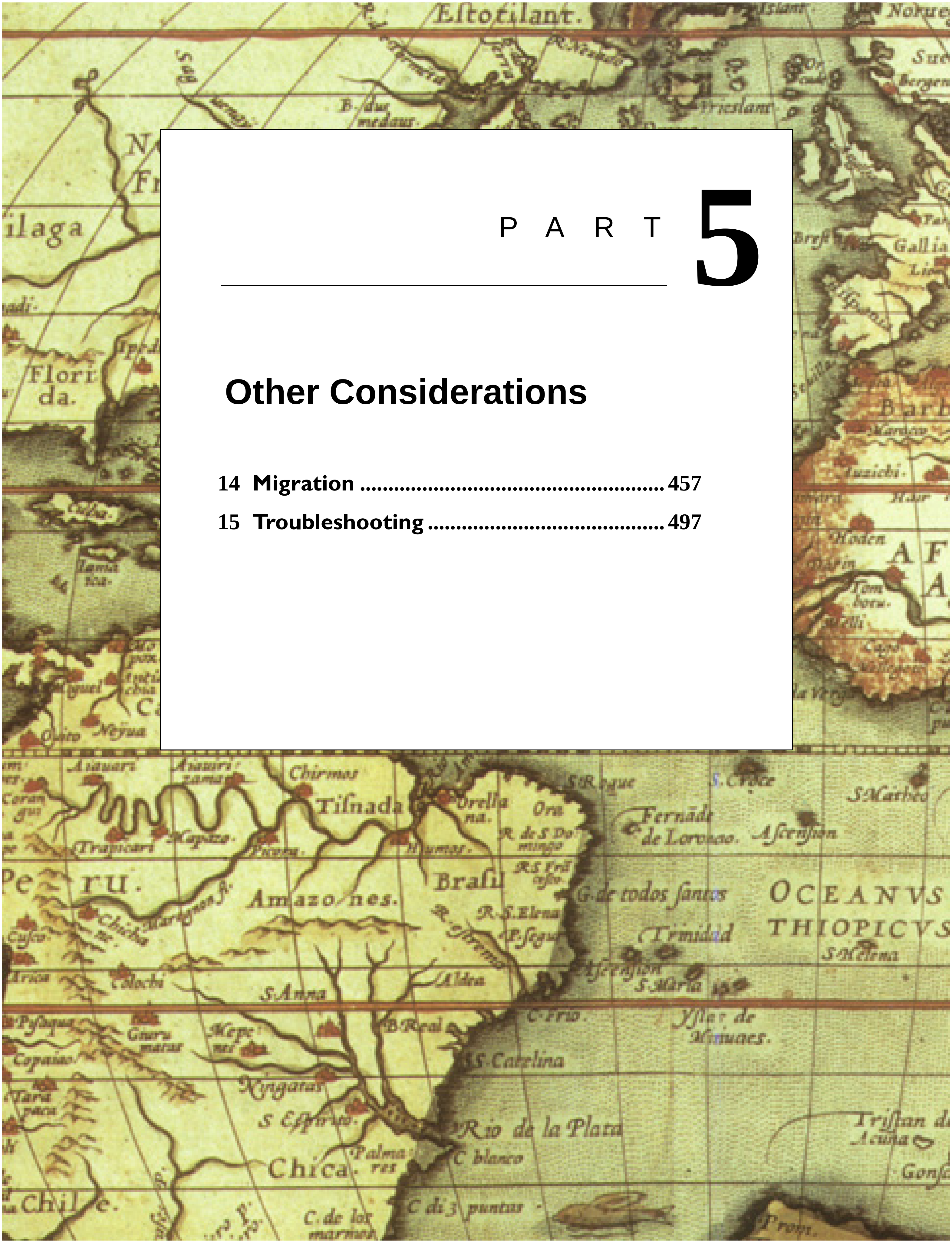
This section has been used to provide a visual example of how the Content Manager eClient enhancements have been implemented to support the new Content Manager data model, text search, and document routing. Table 13–9 lists the Content Manager version 8.1 data model features that the eClient supports.

Table 13–9 *Data Model features supported by the eClient*

Data Model Element	eClient
Attribute	Yes
Attribute Group	Yes
Root Component	Yes
Child Component	One level only
Item type classification[2]	No
Resource item type classification[2]	No
Document item type classification[2]	Yes
Document Part item type classification[2]	Yes
Versions	Yes
Media Object Class	Yes
Item Type Subset[3]	Yes
Semantic Type	Not exposed. Document and folder only.
MIME Type	Yes
Links	Folder only.
References	No
Foreign Keys	No

Notes:
1. Except for BLOB and CLOB types.
2. Item Type Classification

The steps in this section have attempted to identify areas of the eClient that might be represented on the certification exam.



PART 5

Other Considerations

CHAPTER 14

Migration

In this chapter, you will be introduced to Content Manager migration procedures. The following sections will be discussed.

- Setup on Content Manager Version 7.1 Server
- Having Content Manager Version 7.1 Server Ready for Migration
- Installing Content Manager Version 8.1
- Pre-migration
- Testing Migration
- Exporting Metadata by Running Migration Wizard
- Importing Metadata
- Verifying Migration
- Post-migration

Overview

Content Manager version 8.1 provides utilities to assist you in migrating from earlier versions of Content Manager. With these utilities, you can directly migrate data from Content Manager Version 6.1 or Content Manager Version 7.1 on Windows or AIX platform, or VisualInfo or Digital Library Version 2.4 on OS/2, to Content Manager Version 8.1. If you want to migrate from an earlier Content Manager release or product, you must first migrate from that earlier release or product to Content Manager Version 6.1 (if you have it) or Content Manager Version 7.1. For information about migrating from an earlier release to Content Manager Version 6.1, see *Planning and Installation Guide* Version 6.1 (GC26-9831). For information about migrating from an earlier release to Content Manager Version 7.1, see *Planning and Installing Content Manager* Version 7.1 (GC27-0864).

> **Note**: Only Content Manager version 6.1 and version 7.1 can directly migrate to Content Manager version 8.1, on Windows or AIX platform.

Content Manager version 8.1 migration utilities are listed in Table 14–1.

Table 14–1 *Content Manager version 8.1 migration utilities*

Utility	Description
Migration wizard	To export metadata into files.
Icmimpl.exe	To import the data into your Version 8.1 library server
Icmimpo.exe	To import the data into your Version 8.1 resource manager

When you migrate your data to Content Manager Version 8.1, you do not migrate your actual objects or documents, instead, you migrate metadata in your system (both library server and object server(s)) that points to your objects/documents and establishes the structure that you use for finding and retrieving those objects. You use the provided utilities to migrate your system definition data (for example, user IDs, access control lists, and index class definitions) and your user data (for example, attribute values, relationships between items such as folder relationships, and checkout status information).

There are major architectural changes as well as many terminology changes in Content Manager Version v8.1. These have been discussed in the previous chapters of this book. It's essential to understand these changes before migrating your Content Manager system.

Depending on the business requirements, different companies may have different Content Manager, EIP (Enterprise Information Portal) and VideoCharger components in their system. This will lead to different migration strategies when they decide to upgrade to Content Manager version 8.1.

One simple scenario is that a system has one library server, one object server and Window client, and they are all running on the same physical server. This chapter will use this simple scenario to discuss migration procedures. To demonstrate the basic migration procedure, you will migrate a Content Manager version 7.1 server to Content Manager version 8.1 on a Windows NT platform. Assume that Content Manager version 7.1 has been installed and is running properly.

A more complex system may have components of Content Manager and EIP. It may also have customized applications. To upgrade this system to Content Manager version 8.1, you need to perform all the steps which were taken to migrate the previous simple system. Also, you have to consider the upgrade of EIP components. Then, you must modify the customized application to take advantage of new and improved architecture and features.

Content Manager Version 7.1 Server Setup

In order to verify if the migration process completes successfully for discussion purposes, you will create sample data in Content Manager version 7.1 server. When you migrate your production system, this step is not required.

8.1

Note: Do not follow the procedures in this step while migrating your production system.

1. ___ Create key fields

Three key fields are created in Content Manager version 7.1 using the administration client. They are listed in Table 14–2. (Also see Figure 14–1)

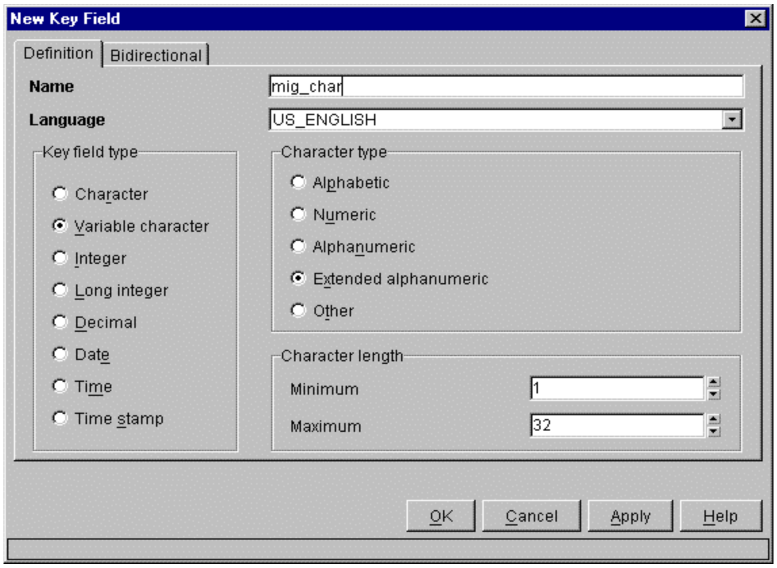
Table 14–2 *Key field definitions in version 7.1*

Name	Characteristic

Mig_char	VARCHAR
	Extended alphanumeric
	Minimum = 1
	Maximum = 32

mig_int	Integer
	Minimum = 1
	Maximum = 1000

mig_date	Date



Name: mig_char

Language: US_ENGLISH

Key field type

○ Character
● Variable character
○ Integer
○ Long integer
○ Decimal
○ Date
○ Time
○ Time stamp

Character type

○ Alphabetic
○ Numeric
○ Alphanumeric
● Extended alphanumeric
○ Other

Character length

Minimum: 1
Maximum: 32

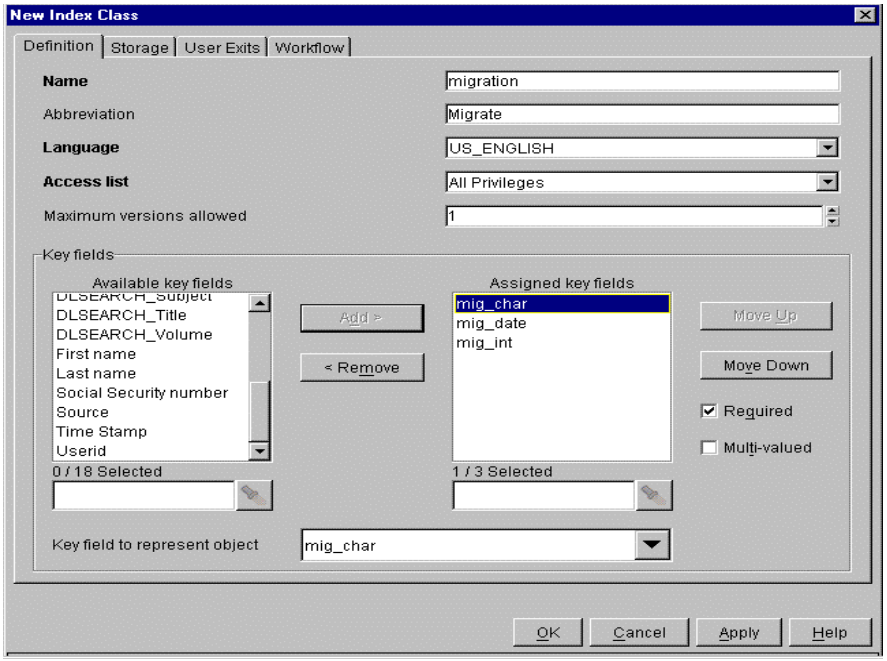
Figure 14–1 *Define key field in version 7.1*

2. ___ Create an index class

The *migration* index class can be created using the Content Manager version 7.1 administration client. It is shown in both Table 14–3 and Figure 14–2.

Table 14–3 *Index class definition in version 7.1*

Field	Value
Name	migration
Abbreviation	Migrate
Language	US_ENGLISH
Access list	All privileges
Maximum versions allowed	1
Key fields	· mig_char, Required, Key field to represent object · mig_date · mig_int
All other fields	Default



Name	migration
Abbreviation	Migrate
Language	US_ENGLISH
Access list	All Privileges
Maximum versions allowed	1

Key fields

Available key fields

DLSEARCH_Subject
DLSEARCH_Title
DLSEARCH_Volume
First name
Last name
Social Security number
Source
Time Stamp
Userid

0 / 18 Selected

Assigned key fields

mig_char
mig_date
mig_int

1 / 3 Selected

☑ Required

□ Multi-valued

Key field to represent object: mig_char

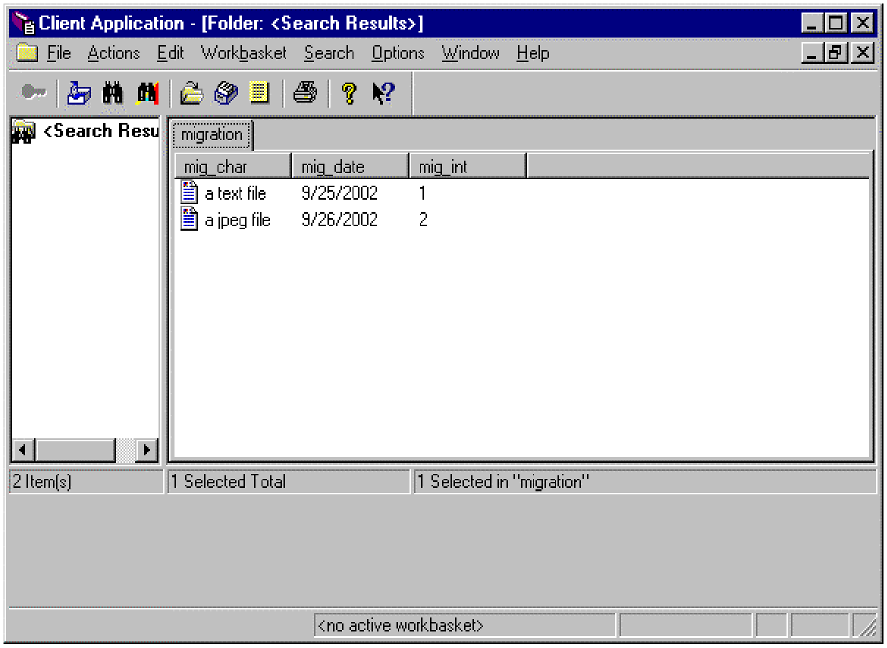
Figure 14–2 *Define index class in version 7.1*

3. ___ Import data

For verification purposes, import two files into Content Manager version 7.1 server using the Windows client. The key fields are defined in Table 14–4. Figure 14–3 shows sample data in version 7.1 Windows client.

Table 14–4 *Import file in version 7.1*

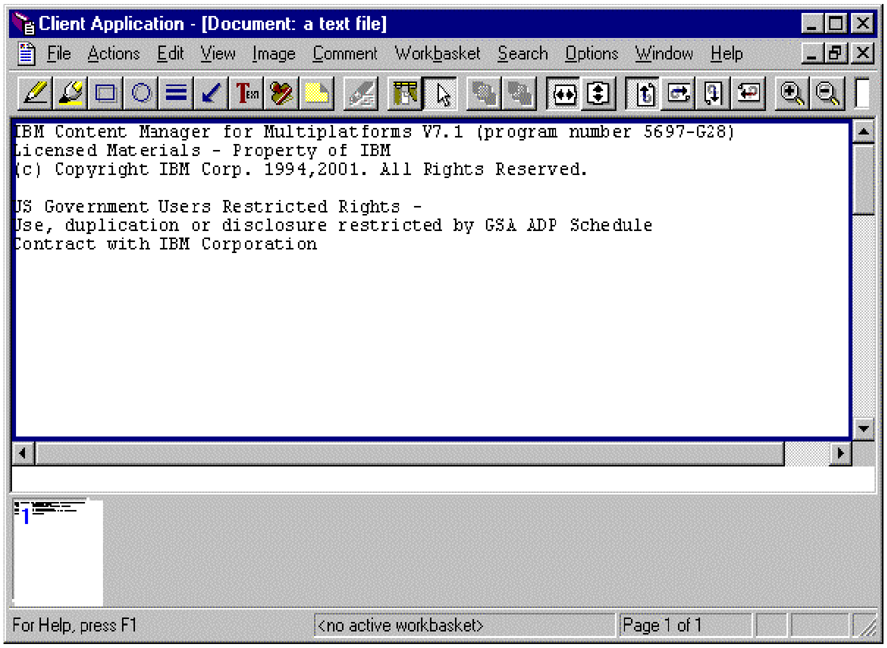
File	mig_char	mig_date	mig_int
#1	a text file	9/25/2002	1
#2	a jpeg file	9/26/2002	2


Client Application - [Folder: <Search Results>]
File Actions Edit Workbasket Search Options Window Help
<Search Resu
migration
2 Item(s)
1 Selected Total
1 Selected in "migration"
<no active workbasket>

mig_char	mig_date	mig_int
a text file	9/25/2002	1
a jpeg file	9/26/2002	2

Figure 14–3 *Search against index class migration in version 7.1*

In Figure 14–4, the content of the imported text file is retrieved in version 7.1 Windows client.


Client Application - [Document: a text file]
File Actions Edit View Image Comment Workbasket Search Options Window Help
For Help, press F1
<no active workbasket>
Page 1 of 1

```
IBM Content Manager for Multiplatforms V7.1 (program number 5697-G28)
Licensed Materials - Property of IBM
(c) Copyright IBM Corp. 1994,2001. All Rights Reserved.

US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule
Contract with IBM Corporation
```

Figure 14–4 *Content of sample file in version 7.1*

Preparing CM Version 7.1 Server for Migration

1. ___ From the Content Manager version 7.1 system administration client, verify that there are no users logged in to the Content Manager server. There should not be any user activities in Content Manager version 7.1 during the migration process.

2. ___ Ensure data integrity. This is critical for any database or content repository.

   - Complete replication if applicable. This ensures all object servers are in the same stage to keep data integrity.

   - This step is not needed for the exercise because you do not have object server replication.

   - Destage all objects in the staging area.

   - This step will ensure that all objects are in proper location (*\lbosdata* directory). In Content Manager version 7.1, an object is first stored in the staging directory while its imported. It is then moved to *\lbosdata* directory by Content Manager process destager.

   - However, this architecture is changed in Content Manager version 8.1.

In version 8.1, the staging directory is not used while importing a document. So, if any imported objects were left in the staging directory without moving to *\lbosdata* directory before migrating to version 8.1, the objects will be lost permanently in the system. This will cause data integrity problems, because the library server shows that they are in the system, but object server can not locate them.

a. Open a DOS command window.

b. Enter **frncmd**. This starts Content Manager version 7.1 command utility.

c. Enter **Connect objdlsrv** to connect to Content Manager version 7.1 object server. Substitute object server name *objdlsrv* with your production server name while migrating your system.

d. Enter **Help** for a list of valid commands.

e. Enter **Destager Start** to start destager process. It will move new imported objects from *\staging* directory to *\lbosdata* directory.

The following are what you should see when running the destager utility.

```
C:\>frncmd
IBM Content Manager for Multiplatforms V7.1 (program number
5697-G28)
Licensed Materials - Property of IBM
(c) Copyright IBM Corp. 1994,2001. All Rights Reserved.
```

```
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Sched-
ule
Contract with IBM Corporation
Enter a command:
        Connect [server name]
        Help
        Listservers
        Quit
>> Connect objdlsrv
FRN2021I: Session Established at 10/07/02 11:59:13 AM
>> Help
Using Server: objdlsrv
Enter a command:
        Status
        Migrator [Status|START|Enable|Disable]
        Destager [Status|START|Enable|Disable]
        Purger   [Status|START|Enable|Disable]
        Replicator   [Status|START|Enable|Disable]
       LIBrary  [Query|Add|Delete] libraryname [VI|DL|ADSM]
userid
        User     [Query|Change_password]  userid
        Trace    [Status|ON|OFF]
        DIsconnect
        Help
        Quit
>> Destager Start
        FRN2027I: Destager running.
```

3. ___ Purge the staging area

Another purpose of the staging directory in Content Manager version 7.1 is to cache objects when they are first retrieved from slow media. You want to remove all cached objects from the staging directory before migration. After migration, Content Manager version 8.1 will handle object caching in its own way.

For this lab, remove all files from **E:\Staging** directory.

4. ___ Stop Content Manager version 7.1 library server, SMS server, and object server to ensure that no users logon during migration and that no objects are migrated outside of the migration that you are beginning.

5. ___ Backup Content Manager version 7.1 system. You should have a fall back plan in case any unexpected evens happen during migration. Having a valid backup of your current production system, will allow you to roll back to Content Manager version 7.1 if the migration failed. You should backup the whole production system, including databases, executable files, system environment, and so on.

Installing Content Manager Version 8.1

1. ___ Make sure that both hardware and software prerequisites for Content Manager version 8.1 are met on the physical server(s).

   If Content Manager version 7.1 library server and Content Manager version 7.1 are running on different physical servers, or there are multiple Content Manager version 7.1 objects server, prerequisites for Content Manager version 8.1 have to be met on all physical servers where version 8.1 components will be installed.

   For this exercise, everything is running on the same physical server.

2. ___ Install Content Manager Version 8.1 library server.

   > **Recommendation**: Install the Version 8.1 library server on a different computer from the version 7.1 library server for adequate disk space.

   Content Manager version 8.1 library server can be installed on the same or a different machine than the version 7.1 library server is running.

   If it is on the same machine as the version 7.1 library server, take the following precautions to ensure that you do not overwrite your existing data:

   a. Use a different name for the Version 8.1 library server database.

   b. Install the Version 8.1 library server in a different directory.

   If you install Version 8.1 on a different machine, it does not need to be on the same operating system as the earlier library server. For example, if you have a Version 7.1 library server on Windows NT, you can migrate to a Version 8.1 library server on AIX.

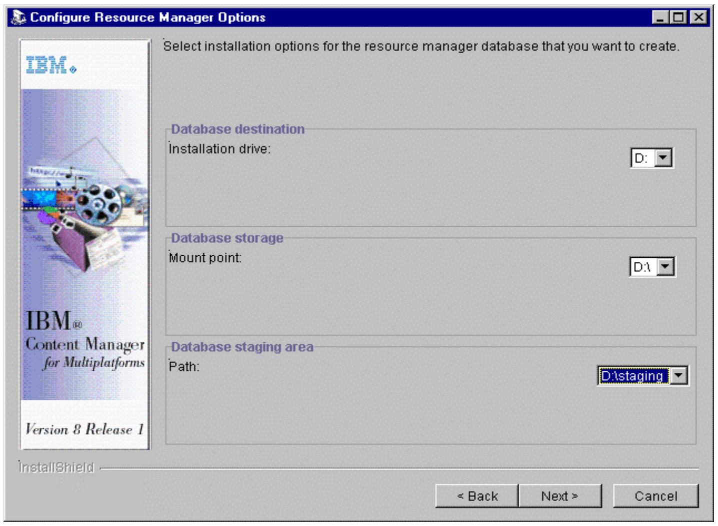
   > **Note**: Do not remove your version 7.1 library servers before installing Version 8.1. Do not overwrite Content Manager version 7.1 library server while installing version 8.1.

3. ___ On the same computer as each of your Content Manager version 7.1 object servers, install one Content Manager Version 8.1 resource manager for each object server.

Note: Do not remove your version 7.1 object servers before installing Version 8.1 resource managers. Do not overwrite your version 7.1 object servers while installing Version 8.1 resource managers.

Note: When you install version 8.1 resource manager, you have to use the same location for both \lbosdata and \Staging directory as they are in version 7.1 system. For example, if your \lbosdata directory in version 7.1 is D:\lbosdata, and staging directory is D:\Staging, you must select D:\ to store object and D:\Staging as staging directory during version 8.1 installation process.

By doing this, Content Manager version 8.1 system will know where your objects are located. Otherwise, you won't be able to retrieve your documents, (see Figure 14–5).



Configure Resource Manager Options

Select installation options for the resource manager database that you want to create.

Database destination
Installation drive: D:

Database storage
Mount point: D:\

Database staging area
Path: D:\staging

Figure 14–5 *Install Content Manager version 8.1*

4. ___ Copy ***\MIGRATE*** directory and its contents from the installation CD to a directory (*c:\migrate*) on your Content Manager version 7.1 library server.

Important: You must have read/write authority in the directory *c:\migrate*. Since *\MIGRATE* directory on Content Manager version 8.1 CD is read-only, you must change its property on version 7.1 library server machine after you copy the whole directory from CD.

This Content Manager version 7.1 library server machine must have:

- Space available for the migration, or it must be attached to a shared drive with enough space. The migration wizard will provide an estimate of the space required.
- A DB2 connection to the Content Manager version 7.1 library server.
- A DB2 connection to the Content Manager version 7.1 object server(s).
- A DB2 connection to the Content Manager version 8.1 library server.
- A jar command (*jar.exe*) in the path for the migration wizard to use.
- A java command (*java.exe*) in the path to start migration wizard.

5. ___ Copy *\MIGRATE* directory and its contents from the installation CD to a directory (*c:\migrate*) on each of your Content Manager version 7.1 object servers.

Important: You must have read/write authority in the directory *c:\migrate*. Since *\MIGRATE* directory on Content Manager version 8.1 CD is read-only, you must change its property on each of version 7.1 object server machines after you copy the whole directory from CD.

This Content Manager version 7.1 object server machine must have:

- Space available for the migration, or it must be attached to a shared drive with enough space.
- A DB2 connection to the Content Manager version 8.1 resource manager.

6. ___ Install the Content Manager Version 8.1 Client for Windows. You might need to do this on many client machines.

- Content Manager version 7.1 clients should continue to be used to access Content Manager version 7.1 servers. End users should continue Content Manager version 7.1 clients until further notice.
- Content Manager Version 8.1 clients now provide access to Version 8.1 servers for testing purposes.

7. ___ Verify Content Manager version 8.1 system is in working condition by performing the following steps:

    a. Create an **attribute**.

    b. Create an **item type**.

    c. **Import** a file into resource manager.

    d. **Search** and **retrieve** the imported file.

Migration and Test

This section discusses the pre-migration process and testing migration.

Pre-Migration

Have the following information ready before the migration process starts:

1. ___ Content Manager version 7.1 library server name. *libdlsrv* is the version 7.1 library server name in this exercise.
2. ___ Content Manager version 8.1 library server name. *icmnlsdb* is the version 8.1 library server name in this exercise.
3. ___ A DB2 Universal Database user name with administrative access privileges and corresponding password for accessing Content Manager version 8.1 library server. Use **icmadmin** and **password** for the demonstration.
4. ___ When you logon to the physical server where the Content Manager version 7.1 library server resides, the logon user ID should be the database owner of the version 7.1 library server database. For this exercise, it is **cmadmin** and **password**.

Testing Migration

Optionally, you could test the migration procedure before migrating your production system. This should smooth your production migration process and is always recommended. You might even consider having multiple dry runs for a large Content Manager system.

Exporting Metadata by Running Migration Wizard

Migration wizard is running on the machine where Content Manager version 7.1 library server resides, to extract metadata stored in both Content Manager version 7.1 library server and object server(s).

> **Note:** While you are completing your final migration, you must migrate all system definition and user data during one migration session so that your data will be synchronized.

Attention: Before beginning the migration, you must confirm the following:

- You have re-booted the Content Manager version 7.1 library server machine. This should prevent any hanging processes from causing problems.
- No users are logged into the Content Manager version 7.1 system.
- The Content Manager Version 7.1 library server, SMS server, and the object server are all stopped.
- The DB2 Universal Database server is running.

1. ___ Logon to the physical server where Content Manager version 7.1 server resides. The logon user ID should be the database owner of version 7.1 library server database. For the exercise, use **cmadmin** and **password**.

2. ___ Open a command window. Your PATH environment variable must contain the directory where java.exe and jar.exe reside. You may confirm this by:

a. Entering **jar.exe** in the command window.

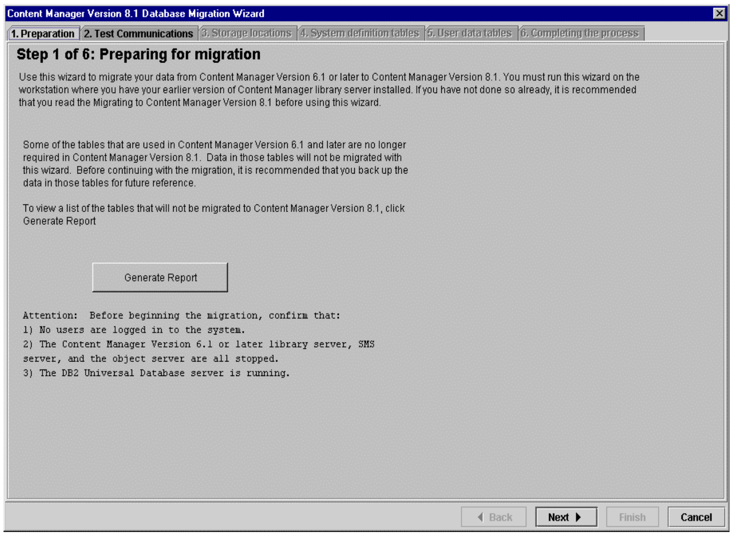
b. Entering **java.exe** in the command window.

3. ___ Change to the directory where you copied the contents of the migration directory. It's **c:\migrate** for the lab.

4. ___ Enter **frn2icml** to start Content Manager Version 8.1 Database Migration Wizard.

5. ___ There are six main panels in Content Manager Version 8.1 Database Migration Wizard. The first one is Step 1 of 6: Preparing for migration.

6. ___ Not all of Content Manager version 7.1 Metadata is required in Content Manager Version 8.1. In step 1 of the wizard, select **Generate Report** to view a list of the database tables that will not be migrated, (see Figure 14–6 and Figure 14–7).



Step 1 of 6: Preparing for migration

Use this wizard to migrate your data from Content Manager Version 6.1 or later to Content Manager Version 8.1. You must run this wizard on the workstation where you have your earlier version of Content Manager library server installed. If you have not done so already, it is recommended that you read the Migrating to Content Manager Version 8.1 before using this wizard.

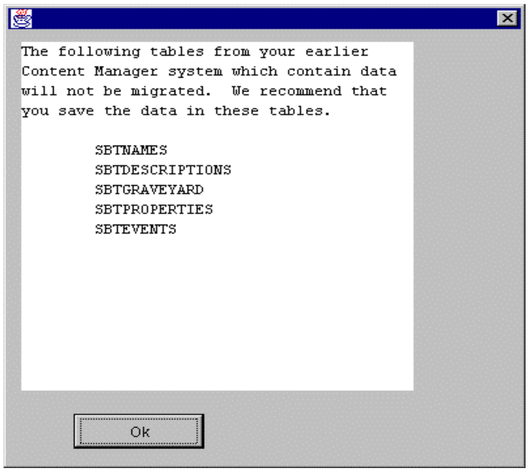
Some of the tables that are used in Content Manager Version 6.1 and later are no longer required in Content Manager Version 8.1. Data in those tables will not be migrated with this wizard. Before continuing with the migration, it is recommended that you back up the data in those tables for future reference.

To view a list of the tables that will not be migrated to Content Manager Version 8.1, click Generate Report

```
Attention:  Before beginning the migration, confirm that:
1) No users are logged in to the system.
2) The Content Manager Version 6.1 or later library server, SMS
server, and the object server are all stopped.
3) The DB2 Universal Database server is running.
```

Figure 14–6 *Step 1of 6: Preparing for migration*

Although you should have the backup of these tables while you backup the whole database, it is recommended to backup the content of these tables separately for easy access.



```
The following tables from your earlier
Content Manager system which contain data
will not be migrated.  We recommend that
you save the data in these tables.

        SBTNAMES
        SBTDESCRIPTIONS
        SBTGRAVEYARD
        SBTPROPERTIES
        SBTEVENTS
```

Figure 14–7 *Tables not migrated by wizard*

7. ___ Select **OK** to close the popup window.

8. ___ Select **Next** and go to Step 2 of 6: Test communication and verify migration authorization panel.

9. ___ In step 2 of the wizard, (see Figure 14–8), enter:

   a. Your Content Manager **version 7.1 library server name**.

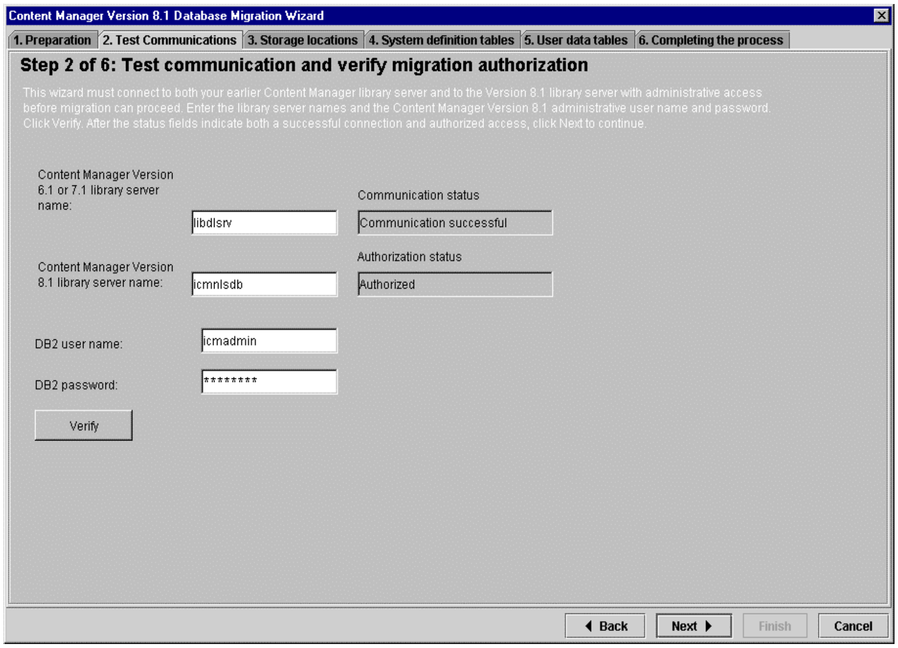
   b. Your Content Manager **version 8.1 library server name**.

   c. A DB2 Universal **Database user name** that has administrative privileges on the Version 8.1 Content Manager library server.

   d. The **password** for the user name. For this exercise, enter values in Table 14–5.

Table 14–5 *Data entered in step 2 of wizard*

Field	Value
Content Manager Version 6.1 or 7.1 library server name	libdlsrv
Content Manager Version 8.1 library server name	icmnlsdb
DB2 user name	icmadmin
DB2 password	password


Content Manager Version 8.1 Database Migration Wizard
1. Preparation
2. Test Communications
3. Storage locations
4. System definition tables
5. User data tables
6. Completing the process

Step 2 of 6: Test communication and verify migration authorization

This wizard must connect to both your earlier Content Manager library server and to the Version 8.1 library server with administrative access before migration can proceed. Enter the library server names and the Content Manager Version 8.1 administrative user name and password. Click Verify. After the status fields indicate both a successful connection and authorized access, click Next to continue.

Content Manager Version 6.1 or 7.1 library server name: libdlsrv

Communication status: Communication successful

Content Manager Version 8.1 library server name: icmnlsdb

Authorization status: Authorized

DB2 user name: icmadmin

DB2 password: ********

Figure 14–8 *Step 2 of 6: Test communication and verify migration authorization*

10. ___ On the same panel, select **Verify** button.

Content Manager version 8.1 migration wizard must connect to both your Content Manager version 7.1 library server and to the version 8.1 library server with administrative access before migration can proceed. Selecting the **Verify** button causes the wizard to check the connection to both version 7.1 server and version 8.1 server. It also validates the provided user name and password has DB2 administrative privileges for version 8.1 library server database.

After the wizard performs verification, it will change the status fields to indicate **communication successful** in the *communication states* field and **authorized** in the *authorization states* field. However, if anything goes wrong, the wizard will display an error code on the panel based on the type of failure.

- If communication fails with the Content Manager version 7.1 library server, the Communication status field displays an *FRNxxxx* error code.
- If communication fails with the Content Manager Version 8.1 library server, the Communication status field displays an SQL error message.
- If authorization fails, verify that the DB2 Universal Database user ID that you entered exists, has administrative privileges, and that the password

you entered is correct.

11. ___ Select **Next** to proceed to Step 3 of 6: *Identify storage location for migration files* panel. In this step, you'll enter a directory to store migration files, (see Figure 14–9).

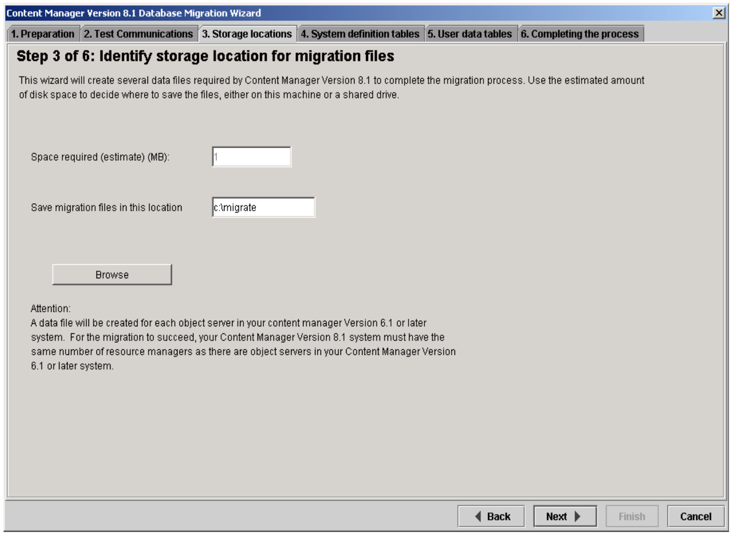
8.1

> **Note**: The directory must pre-exist. If you see an error in the DOS window where the migration wizard was started: *SQL3006C An I/O error occurred while opening the message file*, it means that the directory does not exist.

If you encountered a problem in the migration wizard because the directory is not existing, you need to do the following:

- **a.** Create the directory
- **b.** Cancel the migration process
- **c.** Start the migration wizard again.

12. ___ For the exercise, enter **c:\migrate** and select **Next**. This leads you to the next panel.


Content Manager Version 8.1 Database Migration Wizard
1. Preparation
2. Test Communications
3. Storage locations
4. System definition tables
5. User data tables
6. Completing the process
Browse
Back
Next
Finish
Cancel

Step 3 of 6: Identify storage location for migration files

This wizard will create several data files required by Content Manager Version 8.1 to complete the migration process. Use the estimated amount of disk space to decide where to save the files, either on this machine or a shared drive.

Space required (estimate) (MB): 1

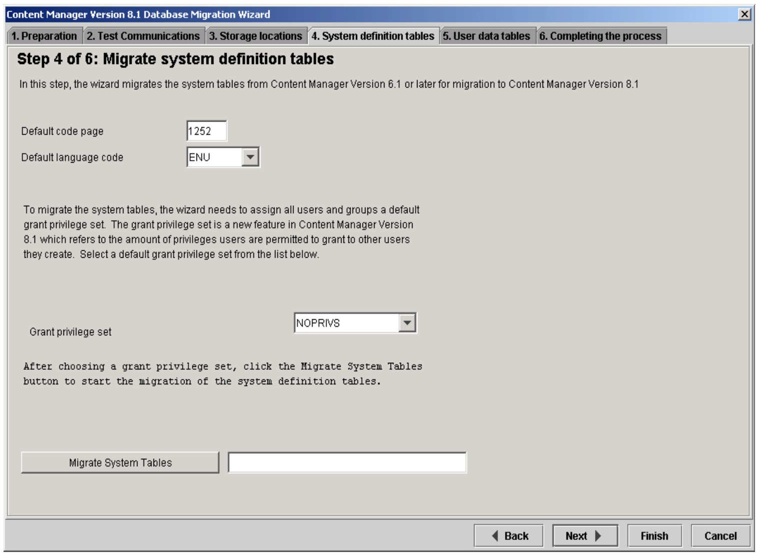
Save migration files in this location c:\migrate

Attention:
A data file will be created for each object server in your content manager Version 6.1 or later system. For the migration to succeed, your Content Manager Version 8.1 system must have the same number of resource managers as there are object servers in your Content Manager Version 6.1 or later system.

Figure 14–9 *Step 3 of 6: Identify storage location for migration files*

13. ___ In step 4 of the wizard, you will migrate system definition tables. Select a **default code page** and **language code**. The code page and language code are for any text notes that were added to documents on your Content Manager version 7.1 object server(s), (see Figure 14–10).

14. ___ For the demonstration, enter 1252 as Default code page and select ENU as Default language code.



Step 4 of 6: Migrate system definition tables

In this step, the wizard migrates the system tables from Content Manager Version 6.1 or later for migration to Content Manager Version 8.1

Default code page 1252

Default language code ENU

To migrate the system tables, the wizard needs to assign all users and groups a default grant privilege set. The grant privilege set is a new feature in Content Manager Version 8.1 which refers to the amount of privileges users are permitted to grant to other users they create. Select a default grant privilege set from the list below.

Grant privilege set NOPRIVS

After choosing a grant privilege set, click the Migrate System Tables button to start the migration of the system definition tables.

Figure 14–10 *Step 4 of 6: Migrate system definition tables*

15. ___ On the same panel, select a default **grant privilege set** for the users that exist in Content Manager version 7.1 system. A *grant privilege set* specifies the privileges that users can grant to users that they will create. Grant privilege sets are a new feature in Version 8.1.

For the exercise, enter **NOPRIVS**.

16. ___ After choosing a grant privilege set, select **Migrate System Tables** button to start the migration of the system definition tables. Content Manager version 7.1 system definition data consists of:

- Language definitions
- Privileges
- Object server definitions
- Collection definitions

- Users
- Groups
- ACLs
- Attributes
- Index classes
- Views
- Workbasket definitions
- Workflow definitions

17. ___ The migration wizard uses the Content Manager Version 8.1 stored procedures to create the Version 8.1 entities. Check the Content Manager Version 8.1 library server log file to see if any error has occurred during this step of the migration process. Also, log files are available in directory c:\migrate, which is entered on Step 3 of 6 wizard panel.

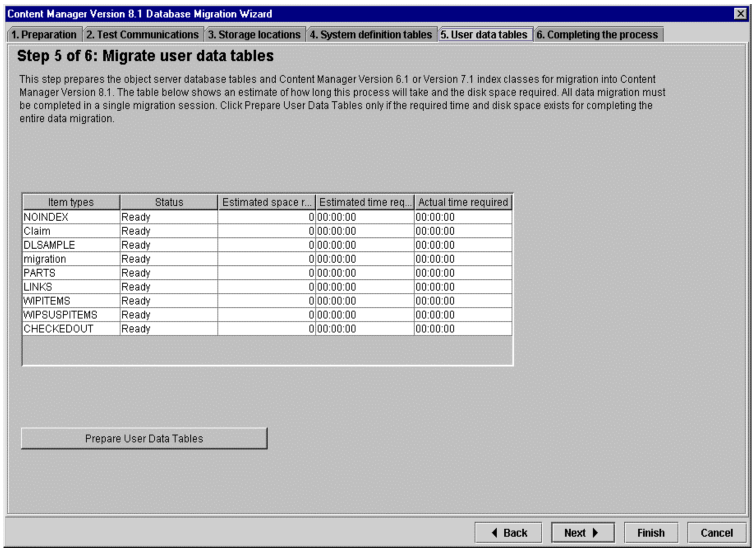
Be patient after selecting Migrate System Tables. The migration may take a couple of minutes.

18. ___ After the system definition table is done, select **Next** and proceed to Step 5 of 6: *Migrate user data tables*.

19. ___ Step 5 of the wizard will migrate your user data. The wizard estimates the amount of time necessary to complete this migration step, which can take a long time to complete, and must be completed in one session (see Figure 14–11).

Before selecting *Prepare User Data Tables*, verify that you have the necessary time to complete the migration before the Content Manager servers must be back in production. At the end of this step, there will be one compressed file for the Content manager version 7.1 library server and one for each version 7.1 object server.

Note: This step prepares the object server database tables and Content Manager Version 7.1 index classes for migration into Content Manager Version 8.1.



Content Manager Version 8.1 Database Migration Wizard
1. Preparation
2. Test Communications
3. Storage locations
4. System definition tables
5. User data tables
6. Completing the process

Step 5 of 6: Migrate user data tables

This step prepares the object server database tables and Content Manager Version 6.1 or Version 7.1 index classes for migration into Content Manager Version 8.1. The table below shows an estimate of how long this process will take and the disk space required. All data migration must be completed in a single migration session. Click Prepare User Data Tables only if the required time and disk space exists for completing the entire data migration.

Item types	Status	Estimated space r...	Estimated time req...	Actual time required
NOINDEX	Ready	0	00:00:00	00:00:00
Claim	Ready	0	00:00:00	00:00:00
DLSAMPLE	Ready	0	00:00:00	00:00:00
migration	Ready	0	00:00:00	00:00:00
PARTS	Ready	0	00:00:00	00:00:00
LINKS	Ready	0	00:00:00	00:00:00
WIPITEMS	Ready	0	00:00:00	00:00:00
WIPSUSPITEMS	Ready	0	00:00:00	00:00:00
CHECKEDOUT	Ready	0	00:00:00	00:00:00

Figure 14–11 *Step 5 of 6: Migrate user data tables*

20. ___ Select **Prepare User Data Tables** button. The wizard starts to migrate user data tables. After the migration is finished for each table, the status should change from *Ready* to *Done*. Upon successful data migration, all tables should have a status of *Done*, (see Figure 14–12).

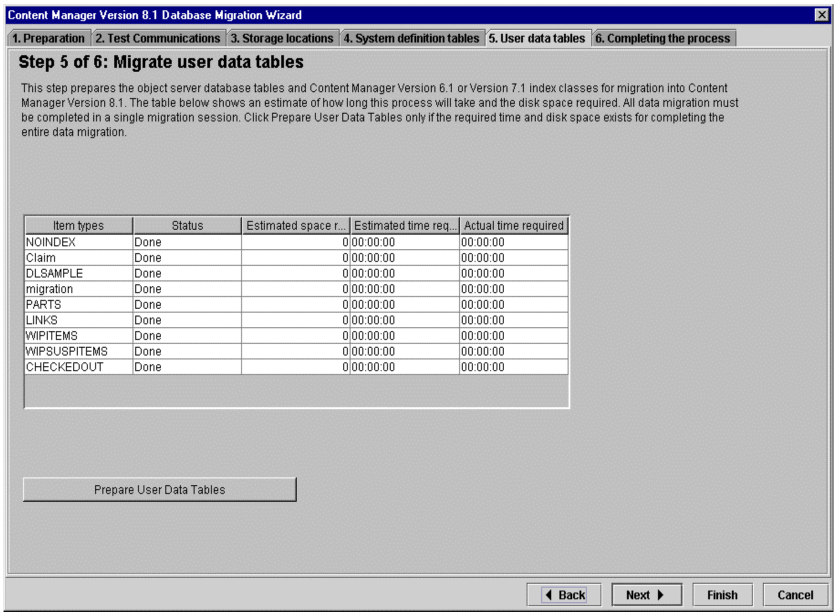
The tables from the Content Manager Version 7.1 system have been converted into compressed data files. The files have been stored in the following directory: *c:\migrate*. You may import the compressed files into Content Manager Version 8.1.

The exported and reformatted data for your Content Manager Version 8.1 system are saved in the following files:

- The library server data is stored in *c:\migrate\icmnlsdb.jar.*
- The object server data is stored in *c:\migrate\objdlsrv.jar.*

If there are multiple object servers in the system, there is one *.jar* file for each of the object servers.

21. ___ Select **Next** for the next panel.



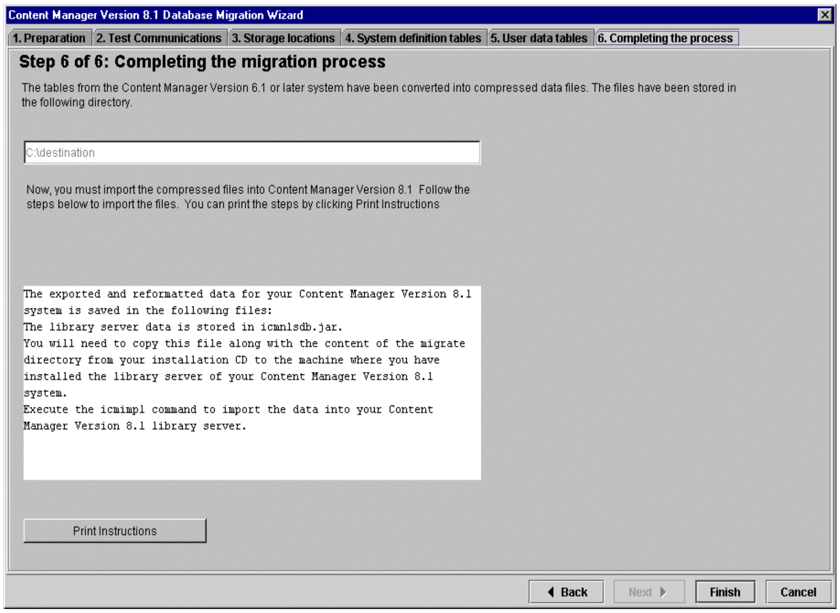
Step 5 of 6: Migrate user data tables

This step prepares the object server database tables and Content Manager Version 6.1 or Version 7.1 index classes for migration into Content Manager Version 8.1. The table below shows an estimate of how long this process will take and the disk space required. All data migration must be completed in a single migration session. Click Prepare User Data Tables only if the required time and disk space exists for completing the entire data migration.

Item types	Status	Estimated space r...	Estimated time req...	Actual time required
NOINDEX	Done	0	00:00:00	00:00:00
Claim	Done	0	00:00:00	00:00:00
DLSAMPLE	Done	0	00:00:00	00:00:00
migration	Done	0	00:00:00	00:00:00
PARTS	Done	0	00:00:00	00:00:00
LINKS	Done	0	00:00:00	00:00:00
WIPITEMS	Done	0	00:00:00	00:00:00
WIPSUSPITEMS	Done	0	00:00:00	00:00:00
CHECKEDOUT	Done	0	00:00:00	00:00:00

Figure 14–12 *User data tables was migrated*

22. ___ In step 6 of the wizard, select **Print Instructions** to print the steps that you must follow to import the compressed, migrated data from the identified directory into Content Manager Version 8.1, (see Figure 14–13).



Step 6 of 6: Completing the migration process

The tables from the Content Manager Version 6.1 or later system have been converted into compressed data files. The files have been stored in the following directory.

C:\destination

Now, you must import the compressed files into Content Manager Version 8.1 Follow the steps below to import the files. You can print the steps by clicking Print Instructions

```
The exported and reformatted data for your Content Manager Version 8.1
system is saved in the following files:
The library server data is stored in icmnlsdb.jar.
You will need to copy this file along with the content of the migrate
directory from your installation CD to the machine where you have
installed the library server of your Content Manager Version 8.1
system.
Execute the icmimpl command to import the data into your Content
Manager Version 8.1 library server.
```

Figure 14–13 *Step 6 of 6: Completing the migration process*

23. ___ Select **Finish** to close the wizard.

Importing Metadata

The migration wizard produces compressed data files in the format *ServerNam*e.jar *(ServerName* is the unique name of the Content Manager version 8.1 library server or version 7.1 object server) and stores them in the directory you specified in step 3 of the wizard. After running the migration wizard, you have one data file for the library server and one for each object server. To complete the migration, follow these steps:

1. ___ Copy the migration directory and its contents from the installation CD to a directory on your Content Manager Version 8.1 library server. You must have read/write authority in the directory on the library server. Since *\MIGRATE* directory on Content Manager version 8.1 CD is read-only, you must change its property on the library server.

   Since you have everything on the same physical machine for this exercise, you do not need to do this step because the directory *c:\migrate* has all the migration components.

2. ___ Copy the migration directory and its contents from the installation CD to a directory on each of your Content Manager Version 8.1 resource managers. You must have read/write authority in the directory on these resource manager servers. Because the *\MIGRATE* directory on Content Manager version 8.1 CD is read-only, you must change its property on the resource manager servers.

   Since you have everything on the same physical machine for this exercise, you do not need to do this step because the directory *c:\migrate* has all the migration components.

3. ___ On each of the corresponding servers, copy one of the *ServerName.jar* files to the directory where you copied the contents of the migrate directory in Step 1 of this procedure.

   Since you have everything on the same physical machine for this exercise, you do not need to do this step because the directory *c:\migrate* has been used as the migration destination.

Note: If you have only one physical server with everything on it, you must do every step in the same directory through the whole migration process. Otherwise, you may encounter problem.

4. ___ On the Content Manager Version 8.1 library server machine,

a. Open a DB2 command window.

b. Change to the directory where you copied the contents of the migrate directory in Step 1 of this procedure. For the exercise, you go to directory **c:\migrate**.

c. Enter **icmimpl 81LibraryServerName User ID Password**

Where

- *Icmimpl* is the command name
- *81LibraryServerName* is the Content Manager version 8.1 library server name which is **icmnlsdb** for this case.
- *User ID* is a user with DB2 administrator authority for *81LibraryServerName*. We use **icmadmin** for the exercise.
- *Password* is the password for *User ID*. For this case, it’s **password**.

This command starts the process to load the data into your Content Manager Version 8.1 library server.

During and after the loading process, you may receive a message, “The system cannot find the path specified.” in your DB2 command window. This message does not indicate any error in your loading process. Please ignore and continue to the next step.

The migration utility has had to perform truncation and character substitution in mapping the Content Manager version 7.1 entity names to the internal names of version 8.1. In version 8.1, you can associate both an internal name and display name to entities such as item types, attributes, and views. During the migration process, the version 7.1 names associated with these entities are mapped to the display name in version 8.1. Due to the restrictions on the length and the character set associated with the internal names of version 8.1, the migration utility performs truncation and character substitution in mapping the version 7.1 names to the internal names of CMv8.1. Specifically, the internal names can only contain alphanumeric characters. If a version 7.1 entity name contained characters other than alphanumeric, those characters are changed to underscore (_). Also, the internal names are limited to 16 characters. So, version 7.1 entity names longer than 16 are truncated. The migration utility creates a log file called transform.log which lists the version 7.1 names and what they are mapped to in version 8.1 during the migration process. You can find this file in c:\migrate directory. You can also view this by looking at the detailed view for item type, attributes, and views in the system administration client program.

5. ___ On each of the Content Manager Version 8.1 resource managers' machine,

   a. Open a DB2 command window.

   b. Change to the directory where you copied the contents of the migrate directory in Step 1 of this procedure. For this exercise, you go to directory **c:\migrate**.

   c. Enter **icmimpo 71ObjectServerName 81ResourceManagerName User ID Password**.

   where

   - *Icmimpo* is the command name
   - *71ObjectServerName* is the Content Manager version 7.1 object server name on this physical server. Enter **objdlsrv** for the exercise.
   - *81ResourceManagerName* is the Content Manager version 8.1 resource manager name which is **rmdb** for this case.
   - *User ID* is a user with DB2 administrator authority for *81ResourceManagerName*. Use **rmadmin** for the exercise.
   - **Password** is the password for *User ID*. For this case, it's **password**.

During the object server database migration, the migration utility creates a table in your CM Version 7.1 object server database and loads data into this table. An error during the loading process might put the tablespace in a locked state and not allow you to access other tables in that tablespace. For that reason it is recommend that you create this new table in a separate tablespace. (The Migration utility prompts and guides you through the creation of the tablespace).

Note: the directory used to create the new table space should pre-exist.

The following is what you should see in DB2 command window while running the command:

```
C:\target>icmimpo  objdlsrv rmdb rmadmin password
```

```
In order to perform the migration of your Object Server to Content
Manager version 8.1 Resource manager, the migration utility will
need to create a temporary table in your Object Server database.
The amount of data stored in this table will be approximately
equal to data in your Object Server's BASE_OBJECTS table. We rec-
ommend that this new table be created in a tablespace different
from the one that you are using for your Object Server tables. You
can either use this utility to create a new tablespace or use an
existing tablespace.
Do you want to create a new tablespace(y/n)
y
enter a directory path where the tablespace should be created
c:\newspace
create tablespace MIGTS MANAGED BY SYSTEM USING ('c:\newspace')
DB20000I  The SQL command completed successfully.
create table cm2icmparts (cmpartid char(44), icmobjectid char(26),
icmmimetype varchar(128), textflag smallint, CMCompID integer,
versionnum integer, userid char(26), rmaccess char(26), lsdbname
varchar(128)) in MIGTS
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The RUNSTATS command completed successfully.
exporting library server table
exporting access table
exporting collections table
exporting devmgr table
exporting mgmt class table
exporting migration transition table
exporting object table
exporting volumes table
exporting storage group class table
exporting storage group volumes table
exporting storage class table
exporting storage group table
exporting sync parm table
exporting sync report table
exporting sync schedule table
exporting sync status table
exporting sync volume table
Objtextparts.del file is zero length
loading demgr table
loading server table
loading access table
loading storage group table
loading mgmt class table
loading collection table
loading storage class table
loading storage group volumes table
loading storage group classes table
loading mig transition table
loading sync schedule table
loading sync status table
loading sync report table
loading sync volume table
loading sync parm table
loading volumes table
loading objects table
 Database Connection Information
 Database server        = DB2/NT 7.2.5
 SQL authorization ID   = RMADMIN
 Local database alias   = RMDB

SQL0100W  No row was found for FETCH, UPDATE or DELETE; or the
result of a query is an empty table.  SQLSTATE=02000
DB20000I  The SQL command completed successfully.
```

Verifying Migration

1. ___ Open the system administration client for both Content Manager version 7.1 and version 8.1, and compare your version 7.1 **key field definition** and version 8.1 **attribute definition**. Keep in mind that version 7.1 key field names may be mapped to new attribute names in version 8.1 as explained in the previous section of this chapter.

For this lab, you have defined three key fields in Content Manager version 7.1. In version 8.1 system administration client, you should find three corresponding attributes. Notice that the display name of an attribute in Content Manager version 8.1 is the same as the name of the key filed in version 7.1. All other characteristics are kept during the migration process. (See Table 14–6 and Figure 14–14)

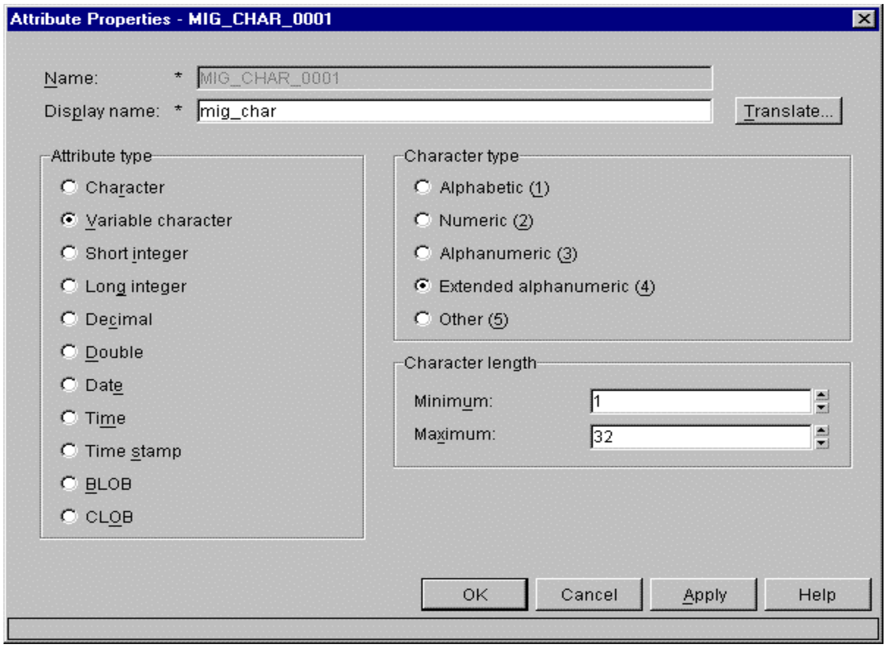
Table 14–6 *Attribute definitions in version 8.1*

Name in version 8.1	Name in version 7.1	Display Name in version 8.1	Characteristic in version 8.1

MIG_CHAR_0001	mig_char	mig_char	VARCHAR
			Extended alphanumeric
			Minimum = 1
			Maximum = 32

MIG_INT_0001	mig_int	mig_int	Short integer
			Minimum = 1
			Maximum = 1000

MIG_DATE_0001	mig_date	mig_date	Date



Attribute Properties - MIG_CHAR_0001

Name: * MIG_CHAR_0001

Display name: * mig_char

Attribute type

- ○ Character
- ● Variable character
- ○ Short integer
- ○ Long integer
- ○ Decimal
- ○ Double
- ○ Date
- ○ Time
- ○ Time stamp
- ○ BLOB
- ○ CLOB

Character type

- ○ Alphabetic (1)
- ○ Numeric (2)
- ○ Alphanumeric (3)
- ● Extended alphanumeric (4)
- ○ Other (5)

Character length

Minimum: 1

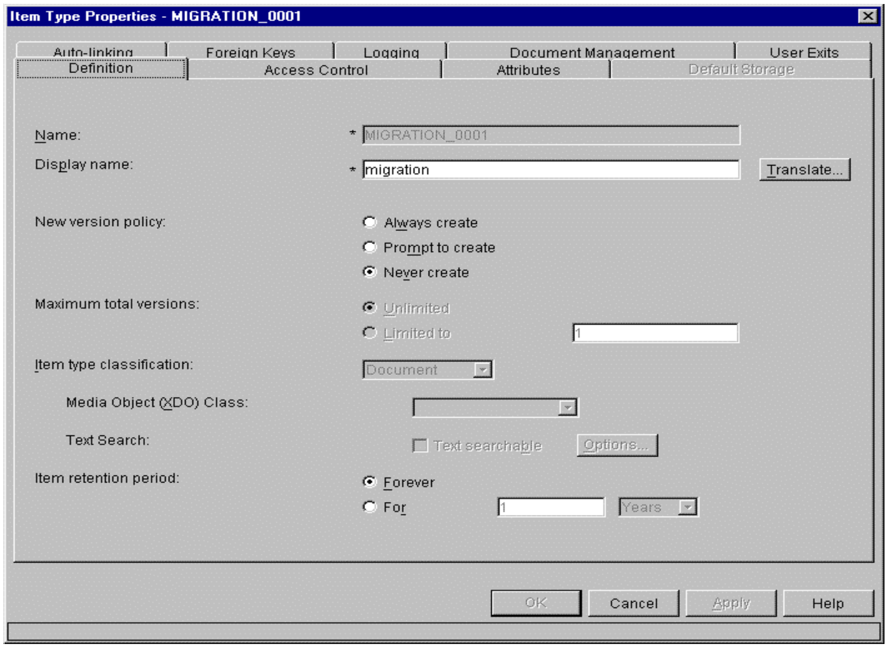
Maximum: 32

Figure 14–14 *Attribute definitions in version 8.1*

For this lab, you have defined one index class in Content Manager version 7.1. In version 8.1 system administration client, you should find one corresponding item type. Notice that the display name of the item type in Content Manager version 8.1 is the same as the name of the index class in version 7.1. All characteristics are kept during the migration process. (See Table 14–7 on page 489, Figure 14–15, Figure 14–16 and Fig. 14–17 on page 491.)

Table 14–7 *Item type definition in version 8.1*

Field	**Value**
Name	MIGRATION_0001
Display Name	migration
Item type classification	Document
Access control list	All privileges
New versions policy	Never create
Key fields	• MIG_CHAR_0001, Required • MIG_DATE_0001 • MIG_INT_0001
All other fields	Default



Name: * MIGRATION_0001

Display name: * migration

New version policy:
○ Always create
○ Prompt to create
● Never create

Maximum total versions:
● Unlimited
○ Limited to 1

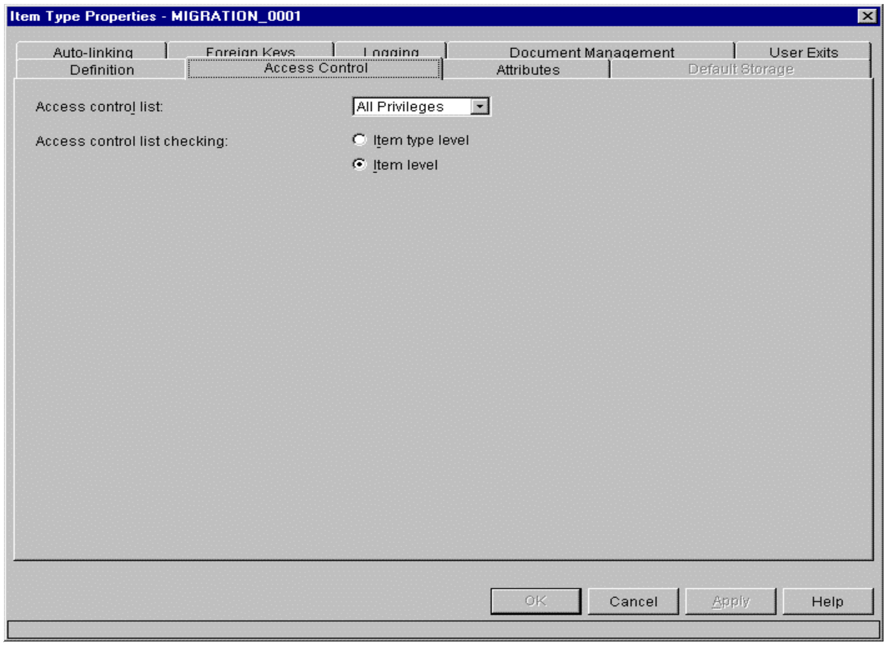
Item type classification: Document

Media Object (XDO) Class:

Text Search: □ Text searchable

Item retention period:
● Forever
○ For 1 Years

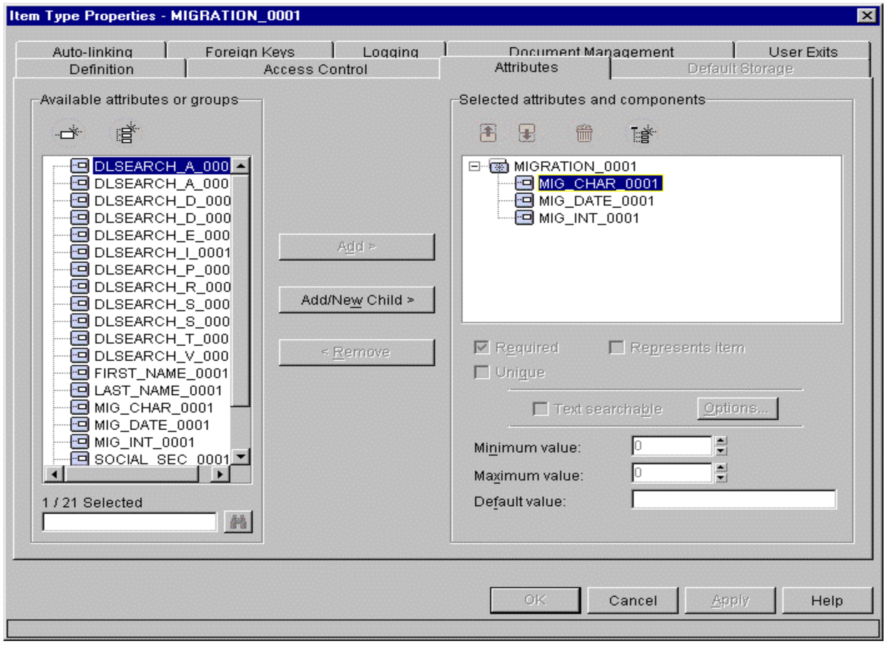
Figure 14–15 *Item type definition in version 8.1*



Access control list: All Privileges

Access control list checking:
○ Item type level
● Item level

Figure 14–16 *Item type definition in version 8.1*


Item Type Properties - MIGRATION_0001

Available attributes or groups:

- DLSEARCH_A_000
- DLSEARCH_A_000
- DLSEARCH_D_000
- DLSEARCH_D_000
- DLSEARCH_E_000
- DLSEARCH_I_0001
- DLSEARCH_P_000
- DLSEARCH_R_000
- DLSEARCH_S_000
- DLSEARCH_S_000
- DLSEARCH_T_000
- DLSEARCH_V_000
- FIRST_NAME_0001
- LAST_NAME_0001
- MIG_CHAR_0001
- MIG_DATE_0001
- MIG_INT_0001
- SOCIAL_SEC_0001

1 / 21 Selected

Selected attributes and components:

- MIGRATION_0001
  - MIG_CHAR_0001
  - MIG_DATE_0001
  - MIG_INT_0001

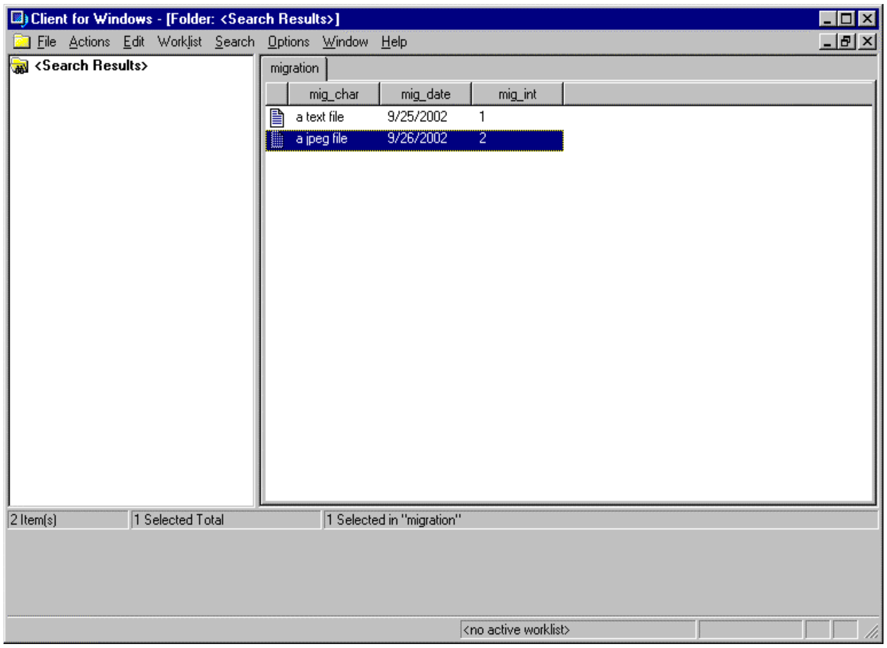
☑ Required ☐ Represents item
☐ Unique
☐ Text searchable Options...

Minimum value: 0
Maximum value: 0
Default value:

Figure 14–17 *Item type definition in version 8.1*

2. ___ Open the Client for Windows for both Content Manager version 7.1 and version 8.1, and **run the same queries** to ensure that your results are as expected. Retrieve objects and make sure that they are accessible and identical.

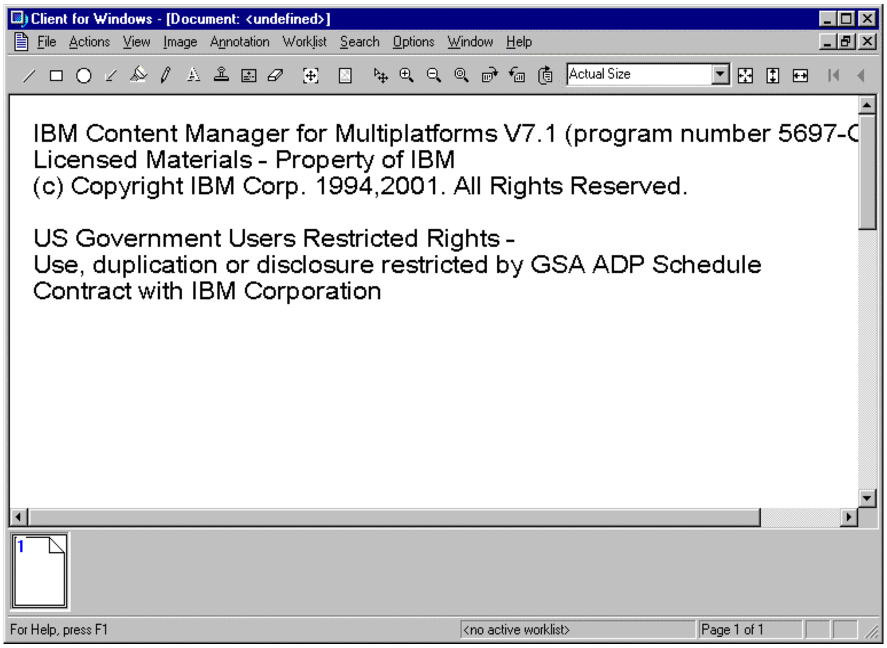
When doing a search against item type *MIGRATION_0001*, you should have the following result as shown in Figure 14–18.


Client for Windows - [Folder: <Search Results>]
File Actions Edit Worklist Search Options Window Help
<Search Results>
migration
2 Item(s)
1 Selected Total
1 Selected in "migration"
<no active worklist>

mig_char	mig_date	mig_int
a text file	9/25/2002	1
a jpeg file	9/26/2002	2

Figure 14–18 *Search against item type MIGRATION_0001 in version 8.1*

3. ___ Retrieve **a text file** document in Content Manager version 8.1 Window client, and compare its content to the one in version 7.1, (see Figure 14–19).


Client for Windows - [Document: <undefined>]
File Actions View Image Annotation Worklist Search Options Window Help
Actual Size
1
For Help, press F1
<no active worklist>
Page 1 of 1

IBM Content Manager for Multiplatforms V7.1 (program number 5697-C
Licensed Materials - Property of IBM
(c) Copyright IBM Corp. 1994,2001. All Rights Reserved.

US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule
Contract with IBM Corporation

Figure 14–19 *Content of sample file in version 8.1*

4. ___ When you migrate a production system, you need to design a more thorough verification test procedure. It’s very important to **verify** the entire migrated system before end users start to use it.

Post Migration

After you have successfully migrated your Content Manager system from version 7.1 to version 8.1, you may want to keep version 7.1 system for a while as a quick fall back plan. However, when your version 8.1 system becomes stable, you may consider removing version 7.1 system.

- (Optional) On the physical server where Content Manager version 7.1 library server resided, remove version 7.1 system, including files and database.
- (Optional) On physical server where Content Manager version 7.1 each object server resided, remove version 7.1 system, including files and database.
- (Optional) On all client workstations, remove Content Manager version 7.1 window client.

Summary

This chapter discussed Content Manager migration procedures. Based on your system environment, you may choose different migration strategies. However, certain common steps have to be taken regardless of your environment. The most basic migration steps for migrating a Content Manager version 7.1 system to version 8.1 were discussed in this chapter.

Content Manager version 8.1 provides utilities to assist you to migrate from earlier versions of Content Manager. With these utilities, you can directly migrate data from Content Manager Version 6.1 or Content Manager Version 7.1 on Windows or AIX platform, or VisualInfo or Digital Library Version 2.4 on OS/2, to Content Manager Version 8.1. If you want to migrate from an earlier Content Manager release or product, you must first migrate from that earlier release or product to Content Manager Version 6.1 (if you have it) or Content Manager Version 7.1.

There are two major steps when migrating Content Manager version 7.1 system to version 8.1. First, you export all metadata in both version 7.1 library server and object server(s) into .jar file. After this step, you should have one *.jar* file for the version 7.1 library server, one *.jar* file for each version 7.1 object server in the system. The utility name is *frn2icml.bat*.

In the next step, you run two utilities to load the exported metadata into Content Manager version 8.1 library server and resource manager(s). The utility to load data into version 8.1 library server is *icmimpl.bat*. The utility to load data into version 8.1 resource manager is *icmimpo.bat*.

The migration utility had to perform truncation and character substitution in mapping the Content Manager version 7.1 entity names to the internal names of version 8.1. During the migration process, the version 7.1 names associated with these entities are mapped to the display name in version 8.1. Due to the restrictions on the length and the character set associated with the internal names of version 8.1, the migration utility performs truncation and character substitution in mapping the version 7.1 names to the internal names of CMv8.1. The migration utility creates a log file called transform.log which lists the version 7.1 names and what they are mapped to in version 8.1 during the migration process. You could find this file in c:\migrate directory. After migration, it’s very likely that you will see different entity names in your system.

CHAPTER 15

Troubleshooting

- Localizing Problem
- Library Server
- Resource Manager
- Clients

In this chapter, you will gain a better understanding of how to troubleshoot problems in a Content Manager system. If you have read the previous chapters, some of the log files and troubleshooting processes mentioned here will be already familiar to you. The intent of this chapter is to provide a focused discussion on what actions should be performed when problems do occur. You will first learn how to localize the problem to a specific area in the Content Manager system. Once the problem has been localized, you will then learn how to trace and resolve it.

Localizing Problem

Understanding the overall architecture of the Content Management system will prove to be very beneficial when troubleshooting errors. One of the first questions you should ask yourself when resolving a problem is, "where in the system is this problem occurring and which components are involved"? A Content Management system involves many software components, some of which include the following:

- DB2 UDB
- DB2 Text Information Extender (TIE)
- WebSphere Application Server
- IBM HTTP Server
- Content Manager library server
- Content Manager resource manager
- Windows Client
- Content Manager eClient

Almost all of these components are related in some way, and either directly or indirectly communicate with each other. For example, when performing a text search from the Windows Client, the Content Manager library server, DB2 UDB, and DB2 TIE components are all used. If the text search fails, you must first determine in which component the failure occurred. This can usually be done by inspecting the error message being returned. In other cases, tracing must be performed.

The library server contains attributes (metadata), text search indexes, document routing information, and access control information. When a client performs a search, the resource manager is not involved. In fact, clients can logon and perform searches (whether they be parametric or text searches) even though the resource manager may not be running.

If you are troubleshooting a problem related to searches or access control, the library server log file would most likely be the first place to begin your investigation. In some situations, you may see error messages containing DB2 UDB return codes. In these circumstances, you should then look in the DB2 UDB Messages and Codes manual for an explanation of why this error would occur.

The resource manager contains information regarding the storage of objects. Being a web application, the way at which you approach a resource manager problem would be different from how you approach a library server problem. Because the resource manager requires a valid token before it honors a request, you must first ensure the library server has generated a valid token for the client. The log files from IBM HTTP Server and WebSphere Application Server must also be used when troubleshooting the resource manager. For example, a problem with the IBM HTTP Server configuration will cause client requests to the resource manager to fail.

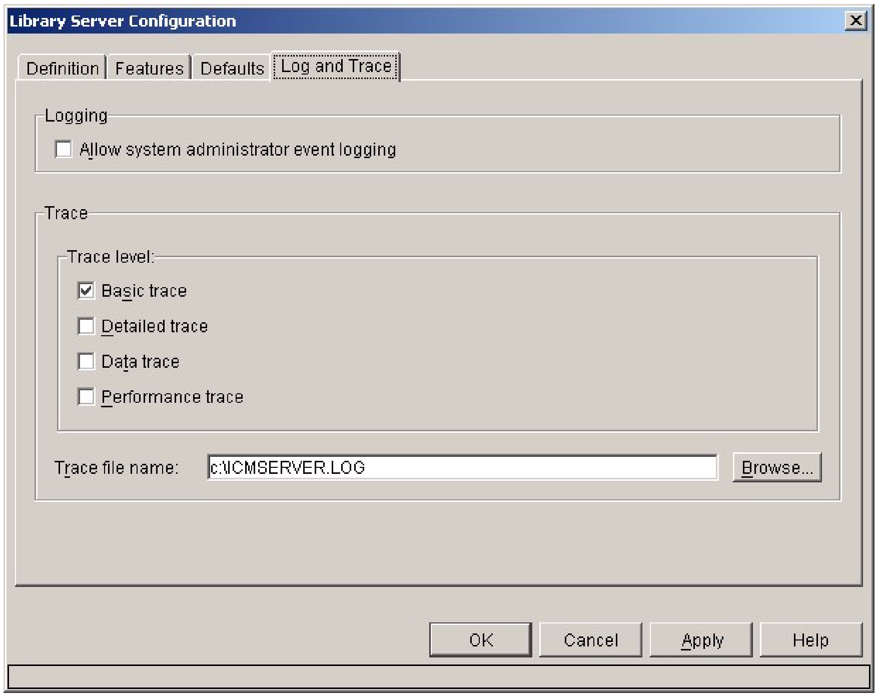
The clients contain their own log files and tracing mechanisms for troubleshooting. However, when errors do arise, you need to be able to determine if the problem originated on the server or on the client. For example, if you get an error message when trying to import a document, you should check both the resource manager and client log files.

In the remainder of this chapter, you will learn how to troubleshoot the library server, resource manager, and clients. Content Manager Version 8.1 involves many components, and contains a great tracing facility. When a problem arises, take a moment to first determine where you should begin your investigation. Doing so usually leads directly to the cause of the error.

Library Server

In this section, you will learn how to troubleshoot problems that involve the library server. The library server is a DB2 UDB database that is accessed by DB2 stored procedures. Recall from the installation exercise that the library server will dynamically generate access modules for item types and static queries. If the access modules cannot be generated, or if there is an underlying problem with the database manager, problems with the library server will occur.

The library server configuration, (see Figure 15–1) allows you to control the level and location of library server tracing. Use the Content Manager System Administration client to update the library server configuration.



☐ Allow system administrator event logging

☑ Basic trace

☐ Detailed trace

☐ Data trace

☐ Performance trace

Trace file name: c:\ICMSERVER.LOG

Figure 15–1 *Updating Library Server Trace Level*

From the Library Server Configuration window, (see Figure 15–1) you can choose various trace levels. Specifically, this window allows you to choose between the following trace levels: basic, detailed, data, and performance. When you change the trace level from the library server configuration window, the TRACELEVEL value in the ICMSTSYSCONTROL table is updated to a corresponding number. The valid tracelevel values are shown in Table 15–1.

Table 15–1 *Library Server Trace Levels*

TRACELEVEL	Description
0	No trace
1	Basic trace: program flow is logged
2	Detail trace: both program flow and data are logged
4	Data trace
8	Performance trace
15	All of the above
16	Build/parse
31	All of the above
32	Memory management
63	All of the above

As you can see from Table 15–1, the tracelevel options shown in the library server configuration window do not represent all possible options. Higher levels of tracing are set by updating the TRACELEVEL value in the library server database table named ICMSTSYSCONTROL.

8.1

Note: A positive tracelevel value will only show what stored procedures are being called. To see what parameter values are being passed, specify a negative tracelevel value. For example, use -63 instead of 63.

From a DB2 Command window (select **Start | Programs | IBM DB2 | Command Window**), issue the following commands to determine what level of tracing the library server is currently set to:

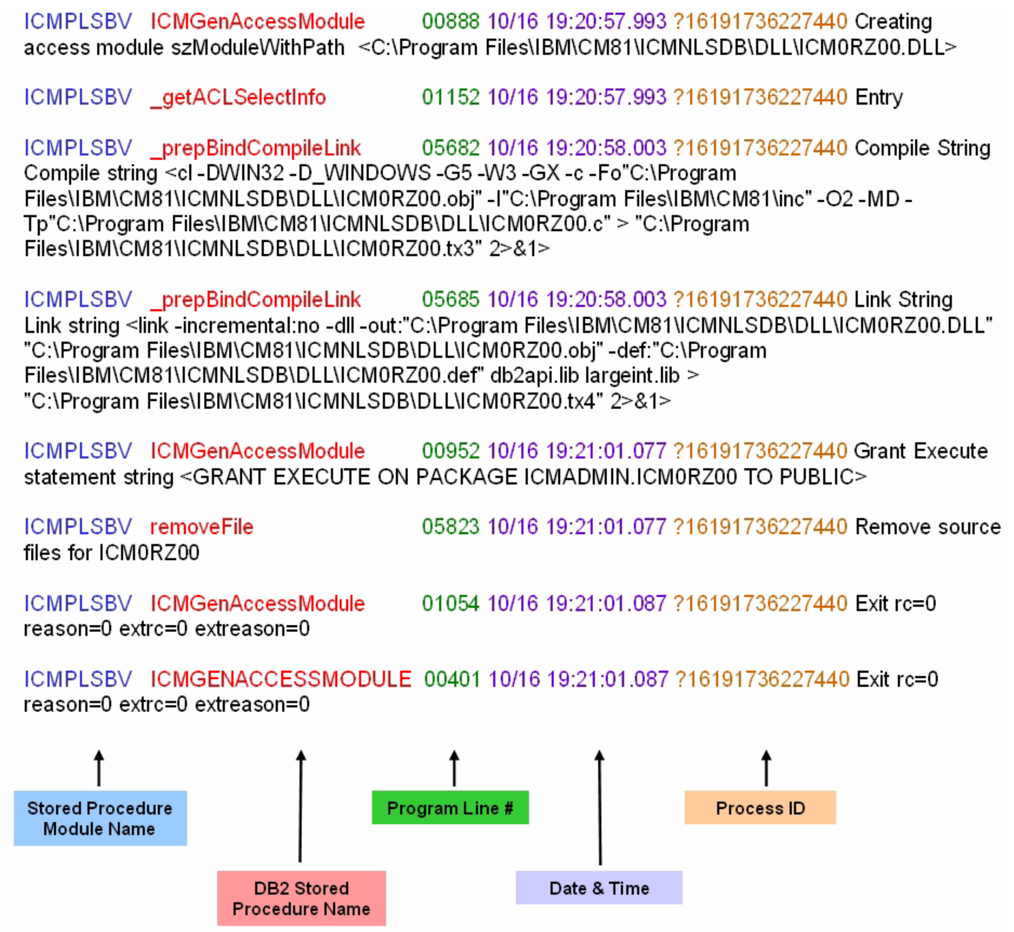
```
db2 connect to icmnlsdb user icmadmin using password
db2 select tracelevel from icmstsyscontrol
```

From a DB2 Command window, issue the following commands to set the library server trace level:

```
db2 connect to icmnlsdb user icmadmin using password
db2 update icmstsyscontrol set tracelevel = <tracelevel>

(where <tracelevel> represents a value from Table 15–1.)
```

By default, the library server traces are placed in the **C:\ICMSERVER.LOG** file. The name and location of this file can also be changed from the library server configuration window, (see Figure 15–1). Depending on the tracelevel value, the ICMSERVER.LOG file will contain different levels of information. However, in all cases, the structure of the log file will remain the same.



```
ICMPLSBV   ICMGenAccessModule       00888 10/16 19:20:57.993 ?16191736227440 Creating
access module szModuleWithPath  <C:\Program Files\IBM\CM81\ICMNLSDB\DLL\ICM0RZ00.DLL>

ICMPLSBV   _getACLSelectInfo        01152 10/16 19:20:57.993 ?16191736227440 Entry

ICMPLSBV   _prepBindCompileLink     05682 10/16 19:20:58.003 ?16191736227440 Compile String
Compile string <cl -DWIN32 -D_WINDOWS -G5 -W3 -GX -c -Fo"C:\Program
Files\IBM\CM81\ICMNLSDB\DLL\ICM0RZ00.obj" -I"C:\Program Files\IBM\CM81\inc" -O2 -MD -
Tp"C:\Program Files\IBM\CM81\ICMNLSDB\DLL\ICM0RZ00.c" > "C:\Program
Files\IBM\CM81\ICMNLSDB\DLL\ICM0RZ00.tx3" 2>&1>

ICMPLSBV   _prepBindCompileLink     05685 10/16 19:20:58.003 ?16191736227440 Link String
Link string <link -incremental:no -dll -out:"C:\Program Files\IBM\CM81\ICMNLSDB\DLL\ICM0RZ00.DLL"
"C:\Program Files\IBM\CM81\ICMNLSDB\DLL\ICM0RZ00.obj" -def:"C:\Program
Files\IBM\CM81\ICMNLSDB\DLL\ICM0RZ00.def" db2api.lib largeint.lib >
"C:\Program Files\IBM\CM81\ICMNLSDB\DLL\ICM0RZ00.tx4" 2>&1>

ICMPLSBV   ICMGenAccessModule       00952 10/16 19:21:01.077 ?16191736227440 Grant Execute
statement string <GRANT EXECUTE ON PACKAGE ICMADMIN.ICM0RZ00 TO PUBLIC>

ICMPLSBV   removeFile               05823 10/16 19:21:01.077 ?16191736227440 Remove source
files for ICM0RZ00

ICMPLSBV   ICMGenAccessModule       01054 10/16 19:21:01.087 ?16191736227440 Exit rc=0
reason=0 extrc=0 extreason=0

ICMPLSBV   ICMGENACCESSMODULE  00401 10/16 19:21:01.087 ?16191736227440 Exit rc=0
reason=0 extrc=0 extreason=0
```

Figure 15–2 *ICMSERVER.LOG Snippet of Access Module Generation*

An example of what you will see in the library server log file when an item type is created is shown in Figure 15–2. In this particular example, the tracelevel was set to detail. This is a very small section of the overall log file, but shows a very important phase of the item type creation process - access module generation. Recall that the Microsoft Visual C++ compiler is used by the library server to dynamically generate access modules for item types and static queries. This example not only shows that the access module generation was successful, but also shows the compile and link commands used to build the dynamic link library (DLL) file.

> 8.1 **Note:** Failing to generate access modules is a very common problem and is usually a result of misconfigured INCLUDE, LIB, and PATH environment variables. The section entitled "Configuring Environment Variables" in Chapter 2 of this guide describes how these variables should be configured.

Each log entry consists of a stored procedure module name, DB2 stored procedure name, program line number, date and time the log entry was made, the process ID (useful when cross referencing DB2 logs), and the description. The point at which a stored procedure is called is logged with an *Entry* message. Likewise, the point at which the stored procedure exits is logged with an *Exit* message. Also note that the return code (rc) is shown when the stored procedure exits. The stored procedure has exited successfully when the return code is equal to zero (rc=0).

The library server log file is an important asset is resolving library server issues. Reasons for not being able to create an item type or unacceptable query performance can be determined by inspecting the library server log file. The maximum trace level is not always needed to investigate a problem. Instead, you should use the minimum tracelevel that gives you enough information to determine the cause of the problem. Doing so will keep you from having to parse through extraneous, and unrelated, log information.

Resource Manager

In this section, you will learn how to troubleshoot resource manager related problems. Configuration errors with WebSphere Application Server and/or DB2 UDB will cause the resource manager to fail. Being able to locate the failing component, and knowing how to correct the problem, is vital in maintaining a resource manager server.

When troubleshooting resource manager related problems, you should keep its architecture in mind. Understanding that the resource manager is a web application is vital in being able to quickly analyze and resolve problems. Being a web application, various components are involved when handling requests. For example, when a client requests a document, the library server, web server, and resource manager web application are all involved. You need to use the log files generated by each of these components in order to troubleshoot problems.

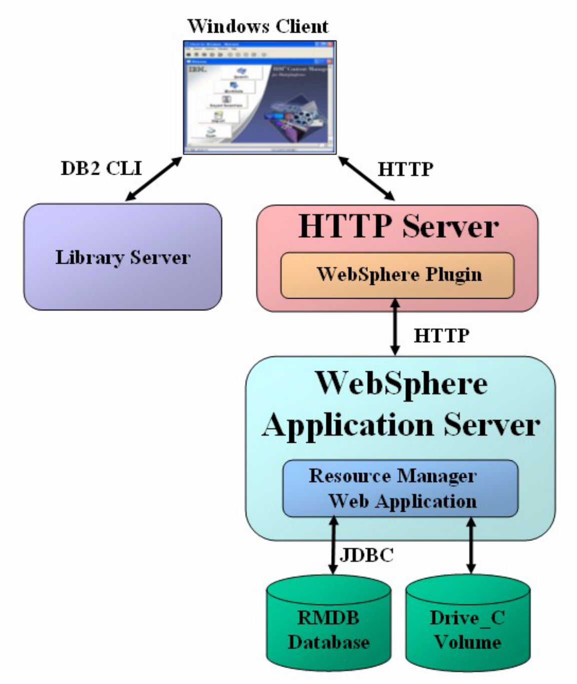


Figure 15–3 *Components Involved in Resource Manager Troubleshooting*

Referencing the system configuration depicted in Figure 15–3 is useful when investigating a problem with the resource manager. A client must first obtain a token from the library server. (Once a token is obtained, it can be reused by the client until it expires.) The client passes its request and this token to the HTTP Server. The WebSphere Plug-in (running inside the HTTP Server) will forward the request to the resource manager web application (running inside of WebSphere Application Server). The resource manager web application will first decrypt and validate the token. Lastly, depending on the type of request, information will either be read from or stored into the resource manager database (i.e. RMDB) and file system volume (i.e. Drive_C).

> **Note:** When accessing the resource manager from the Content Manager System Administration Client, SSL must be properly configured since HTTPS is used instead of HTTP. However, SSL is NOT required when using the Windows Client to retrieve and store documents.

In the remainder of this section, you will learn how to systematically troubleshoot the resource manager. The points which will be discussed include the following:

- Verify database creation
- Verify database connections
- Verify resource manager deployment
- Verify communication with web server
- Resource manager logging
- Secured Sockets Layer (SSL)

Verify Database Creation

If a new installation has been performed, and the resource manager is not functioning properly, you should ensure that the resource manager database was created successfully. Recall from the installation exercise in Chapter 3 that the resource manager database creation log is named icmcrrmdb.log and is located, by default, in C:\Program Files\IBM\CM81\logs.

Review this file closely to be sure that all SQL commands were completed successfully. You must distinguish between error and warning messages, as both are contained in this log file. A common mistake is to forget to grant the necessary database authority to the resource manager userid. This would result in the following message to be logged: *RMADMIN does not have the privilege to perform operation*.

After correcting any problems, you can recreate the resource manager database by selecting **Start | Programs | IBM Content Manager for Multiplatforms V8.1 | Resource Manager Database Install**.

Verify Resource Manager Deployment

Being able to verify that the resource manager web application has been successfully deployed is vital in resolving resource manager installation problems. If the web application was not installed properly, or if the web server plugin was not regenerated, then the resource manager server will be unresponsive.

As Figure 15–4 depicts, a client can access the resource manager web application (icmrm) in two ways. The first is the default method of going through the web server (i.e. IBM HTTP Server). In this case, a request to port 80 is made by http://server/icmrm/snoop. The web server plugin will forward the request to WebSphere Application Server (WAS). The second method is to send the request directly to WAS by specifying the port the application server instance is listening on (i.e. http://server:9080/icmrm/snoop).

Troubleshooting

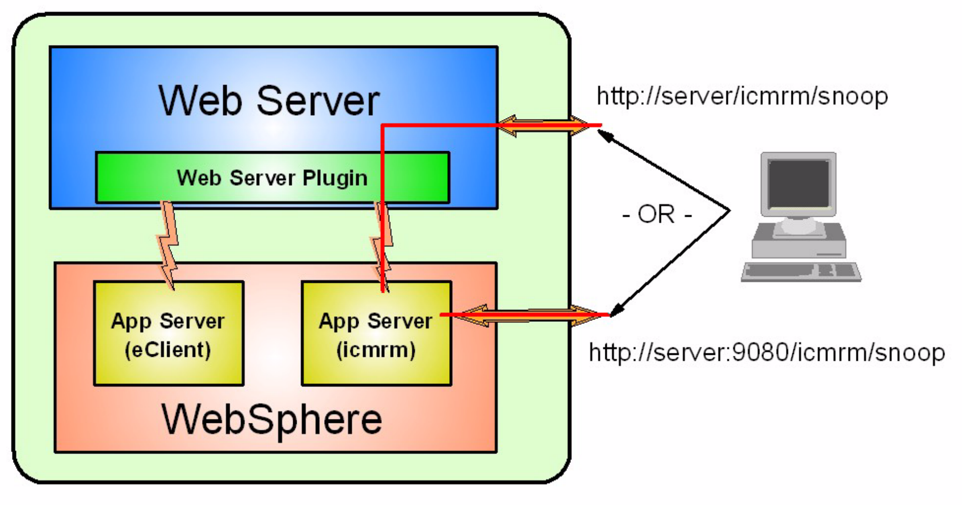


Figure 15–4 *Web Server Integration With WebSphere Application Server*

If the direct method (http://server:9080/icmrm/snoop) fails, then either the resource manager web application is not started, or has not been properly deployed. In this circumstance manually deploying the resource manager web application may resolve the problem.

Note: The section entitled *Managing the Resource Manager* in Chapter 9 of this guide contains instructions on how to manually deploy the resource manager..

If the direct method is successful, but going through the web server (http://server/icmrm/snoop) fails, then the problem lies with the web server plug-in. In this circumstance, regenerating the web server plug-in (done via the WebSphere Administrative Console) will usually resolve the problem.

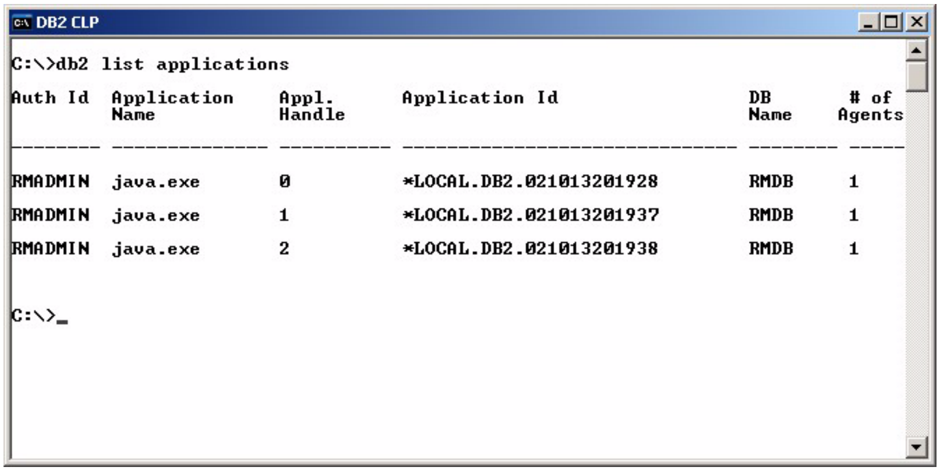
Note: The WebSphere standard error log file may also contain error messages related to the resource manager deployment and operation. The standard error log file is located, by default, in C:\WebSphere\AppServer\logs.

Verify Database Connections

When the resource manager web application starts, it will attempt to connect to the resource manager database (RMDB). If this database connection cannot be made, the resource manager will be unable to handle client requests.

Note: When the resource manager starts, it will make 3 connections to the resource manager database (RMDB).

To validate that the database connections are active, run **db2 list applications** from a db2 command window. Three connections to the resource manager database should appear, (see Figure 15–5).



```
C:\>db2 list applications

Auth Id  Application    Appl.      Application Id                 DB       # of
         Name           Handle                                    Name     Agents
-------- -------------- ---------- ------------------------------ -------- -----

RMADMIN  java.exe       0          *LOCAL.DB2.021013201928        RMDB     1

RMADMIN  java.exe       1          *LOCAL.DB2.021013201937        RMDB     1

RMADMIN  java.exe       2          *LOCAL.DB2.021013201938        RMDB     1


C:\>_
```

Figure 15–5 *Resource Manager Connect to Database*

If the connections do not appear, then the resource manager web application is having a problem connecting to the database. Usually, this occurs when the user ID and password used by the resource manager to connect to the database are invalid. The user ID and password information are stored in the icmrm.properties file (located in C:\WebSphere\AppServer\installedApps\icmrm.ear\icmrm.war\WEB-INF\classes\com\ibm\mm\icmrm). Validate the values for the DBUserid and DBPassword parameters. (Enter the password as plain text, and the resource manager will re-encrypt it.) The user ID and password entered here can be tested by issuing the following command from a DB2 Command Window: **db2 connect to rmdb user <*userid*> using <*password*>**.

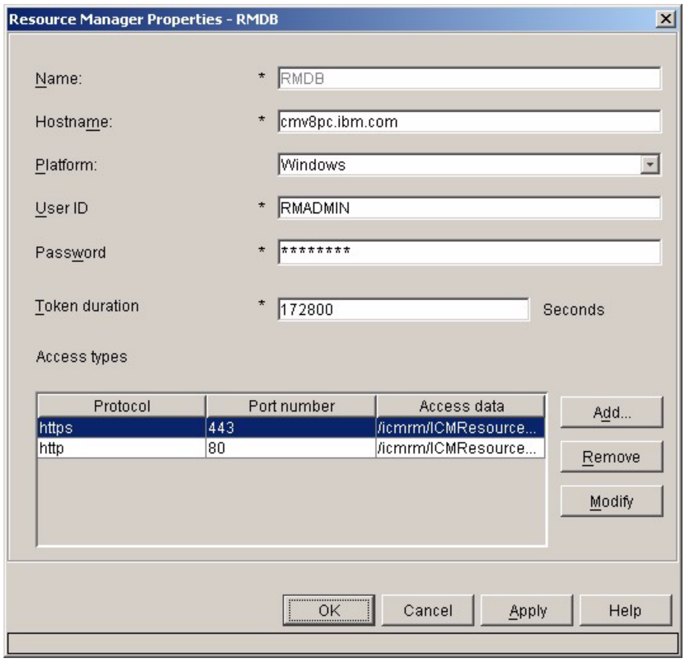
Database connections will also fail if the db2java.zip file is not in the WebSphere Application Server classpath. In this circumstance, the WebSphere Application Server standard error log file will contain a message indicating that the DB2 JDBC driver could not be found.

Verify Communication With Web Server

If the resource manager hostname was incorrectly specified during the install (or if the resource manager hostname has changed), a client request will never reach the web server. By default, the IBM HTTP Server will log every client request in the **C:\IBM HTTP Server\logs\access.log** file. This file can be used to verify the resource manager URL and that the client request is getting to the web server. The following lines are an example of what you will see in the access.log file when a client imports a document:

```
192.168.1.1 - - [19/Oct/2002:19:04:48 -0500] "POST /icmrm/
ICMResourceManager HTTP/1.1" 200 1171
192.168.1.1 - - [19/Oct/2002:19:04:51 -0500] "POST /icmrm/
ICMResourceManager HTTP/1.1" 200 413
192.168.1.1 - - [19/Oct/2002:19:04:54 -0500] "POST /icmrm/
ICMResourceManager HTTP/1.1" 200 403
```

The URL used by the client to access the resource manager can be configured from the Content Manager System Administration Client. Choosing a resource manager and selecting its properties will display the window shown in Figure 15–6. From this window, you can specify the hostname, port, and URL path.



Name: * RMDB

Hostname: * cmv8pc.ibm.com

Platform: Windows

User ID * RMADMIN

Password * ********

Token duration * 172800 Seconds

Access types

Protocol	Port number	Access data
https	443	/icmrm/ICMResource...
http	80	/icmrm/ICMResource...

Figure 15–6 *Resource Manager Properties*

Resource Manager Logging

The resource manager will log errors into the log file named **icmrm.logfile**. This file is located, by default, in C:\Program Files\IBM\CM81\logs. In addition to the default log file, the resource manager contains a logging facility that is based upon Log4J (an open source project available from apache.org). The logging facility consists of various xml files, each of which controls the level and location of logging for different parts of the resource manager server. A description of these log files can be found in Table 15–2.

Table 15–2 *Resource Manager Logging Control Files*

Filename	Description
icmrm_async_logging.xml	Logging control for async recovery utility
icmrm_logging.xml	Logging control for resource manager servlets
icmrm_migrator_logging.xml	Logging control for migrator

Table 15–2 *Resource Manager Logging Control Files*

Filename	Description
icmrm_purger_logging.xml	Logging control for purger
icmrm_stager_logging.xml	Logging control for stager

By default, the resource manager logging control files are located in C:\WebSphere\AppServer\installedApps\icmrm.ear\icmrm.war. Problems can be traced by adjusting the logging level in the respective xml file.

To trace a problem, open a logging control file and locate the following two lines (located towards the end of the file):

```
<priority value="INFO" class="com.ibm.mm.icmrm.util.ICMRMPriority"/>
<appender-ref ref="ASYNC"/>
```

These are the only two lines that you need to change. The priority parameter specifies the level of tracing. The valid priority values are described in Table 15–3:

Table 15–3 *Resource Manager Logging Priority Values*

Priority Value	Description
FATAL	Only log if the servlet is terminating unexpectedly.
ACTION	Messages that describe an action the System Administrator needs to take. These are not errors but conditions such as being short on space.
ERROR	Indicates a request was unable to be fu filled or an internal error.
WARN	Warnings of unexpected behavior.
INFO	Informational start/stop messages.
BEGINEND	Time markers begin and end for performance measures.
REQUEST	Detailed information on the incoming request.
RESPONSE	Detailed information on the outgoing request.
TRACE	General flow messages.
DEBUG	Detailed debugging information, plus all other levels.

Note: Increasing the priorty value will negatively impact the performance of the resource manager.

For example, if you wanted to log all possible information, you would update the priority tag to look like:

```
<priority value="DEBUG" class="com.ibm.mm.icmrm.util.ICMRMPriority"/>
```

The appender-ref parameter specifies where log messages are written. The valid appender-ref values are described in Table 15–4.

Table 15–4 *Resource Manager Logging Appender-ref Values*

Appender-ref Value	Description
FILE	Messages are sent to a log file. The filename is specified in the FILE stanza (located toward beginning of xml file). By default, the file will be placed in the \WebSphere\AppServer\logs directory.
WRAP	Messages are sent to a circular log file (after the file reaches a maximum size, the oldest messages are removed to make room for the most recent messages). By default, the file will be placed in the \WebSphere\AppServer\logs directory.
CONSOLE	Messages are sent to standard output, which ends up in the WebSphere log files.
ASYNC	Messages are sent to standard output, which ends up in the WebSphere log files. While this is faster than CONSOLE, it does not include file and line number information in its messages.

For example, to send messages to a log file in the \WebSphere\AppServer\logs directory, the appender-ref tag should look like either one of the following:

```
<appender-ref ref="FILE"/>
```

```
<appender-ref ref="WRAP"/>
```

The log filename will consists of **icmrm.<component>.logfile**, where <component> is the resource manager process that is writing to the logfile.

For example, icmrm_migrator_logging.xml will create a file named icmrm.migrator.logfile.

In addition to the logging facility, the resource manager provides an administrative servlet. To access this servlet, open a web browser and go to *https://<hostname>/icmrm/ICMRMAdminServlet*, where <hostname> is the name of your machine. (SSL connections do not work with the localhost hostname.) Login as **rmadmin**, using **password** as the password. From this browser interface, you can update the resource manager configuration and view the object storage configuration.

Secured Sockets Layer (SSL)

A secured sockets layer (SSL) is only required to perform resource manager configuration. Therefore, if you are having problems importing or retrieving documents, you safely conclude SSL is not the cause. If you are trying to access the resource manager from the System Administration Client, and are receiving an error, then SSL may be suspect.

Steps to configure SSL can be found in Chapter 3 of this guide. Recall that you must create a self-signed certificate and configure the web server for use with SSL. Also, if you are using WebSphere Application Server AE, you must add *.443 as a virtual host alias (done via the WebSphere Administrative Console).

As Figure 15–7 shows, you can use your web browser to test the SSL configuration at various points in the system. Before troubleshooting SSL, be sure that your resource manager is operating properly. This can be accomplished by either importing or retrieving a document.

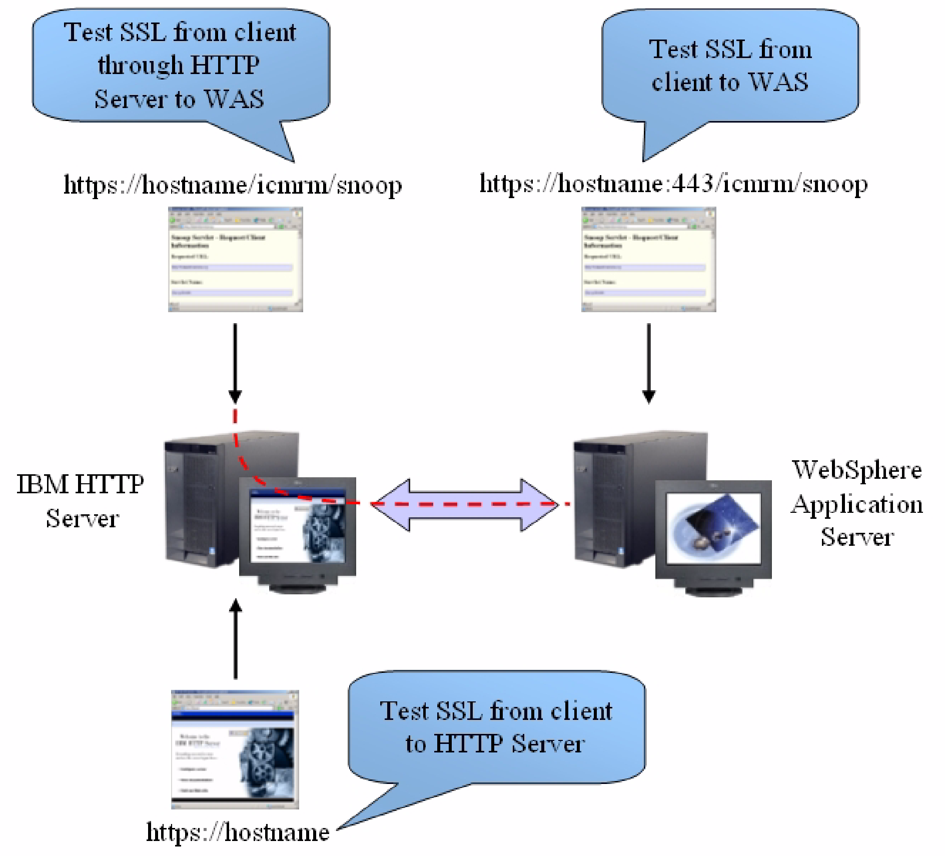

Test SSL from client through HTTP Server to WAS
Test SSL from client to WAS
https://hostname/icmrm/snoop
https://hostname:443/icmrm/snoop
IBM HTTP Server
WebSphere Application Server
Test SSL from client to HTTP Server
https://hostname

Figure 15–7 *Troubleshooting SSL Problems*

Once you have verified the resource manager configuration, open a web browser and go to *https://<hostname>*, where *<hostname>* is the hostname of your web server. Note that https is used instead of http. After accepting the self-signed certificate you created during the SSL configuration, the IBM HTTP Server welcome page should appear. If you instead get an error message, check the IBM HTTP Server log file named **error.log** for SSL related error messages. This log file is located, by default, in C:\IBM HTTP Server\logs.

Note: When working with SSL, never specify *localhost* as the hostname. SSL requires that you use a valid machine hostname.

After verifying the SSL connection between the client and HTTP server, you should then validate the SSL connection between the client and WebSphere Application Server. In this case, you must specify the default SSL port of 443. This is accomplished by opening a web browser and going to *https://<hostname>:443/icmrm/snoop*. If this fails, be sure to check the WebSphere Application Server log files which are located, by default, in C:\WebSphere\AppServer\logs.

8.1

Note: If using WebSphere AE, you must manually add the SSL port of 443 to the list of virtual hosts in the WebSphere Administrative Console. Instructions for doing so can be found in the publication entitled *Planning and Installing Your Content Management System (GC27-1332)*.

Lastly, you should verify the SSL connection is working when communicating from the client, through the web server, to WebSphere Application Server. This is accomplished by opening a web browser and going to *https://<hostname>/icmrm/snoop*. If this fails, you should check the IBM HTTP Server log files which are located, by default, in C:\IBM HTTP Server\logs.

Clients

In this section, you will learn how to troubleshoot problems relating to the Windows Client and eClient. Log files and the procedure for performing tracing will be discussed. Analyzing these traces and error logs will help you determine where the error originated.

Windows Client

The Content Manager Windows Client is built with the C++ Object Oriented API Toolkit. In most circumstances, a Windows Client will either have a problem connecting to the library server or accessing a resource manager. As Figure 15–8 shows, the connection to the library server is made using the DB2 Runtime Client.

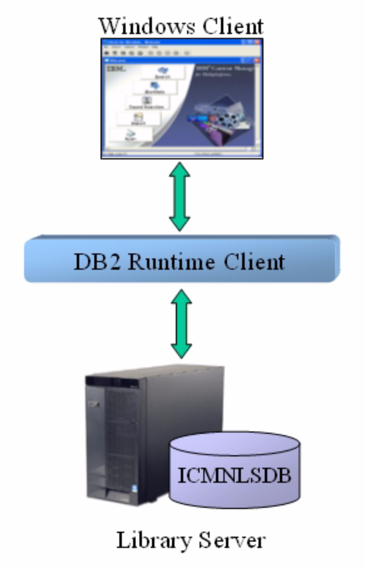


Figure 15–8 *Windows Client Connecting to Library Server*

Recall from the discussion about Content Manager user IDs in Chapter 3, that two connections are made when a client logons to a library server. The first is the physical database connection to the ICMNLSDB. The second is the logical connection to Content Manager (where the supplied user ID and password is authenticated with what is stored in the ICMSTUSERS table.)

In order for the database connection to be made, the library server database must be cataloged on the client workstation (which is why the DB2

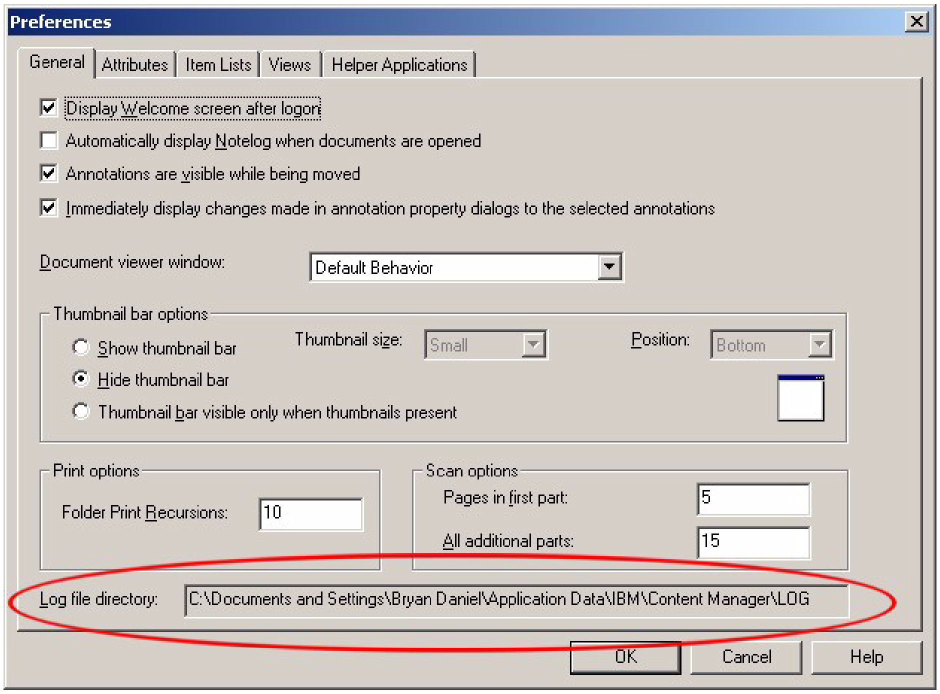
Runtime Client is needed). To check if the library server database has been cataloged on the client machine, go to a DB2 Command Window (**Start | Programs | IBM DB2 | Command Window**) and enter **db2 list database directory**. The library server database should appear. If you do not see the database listed, you can use the DB2 Client Configuration Assistant (**Start | Programs | IBM DB2 | Client Configuration Assistant**) to catalog the database on the client machine.

8.1

Note: To have the APIs automatically catalog the database on a client machine, *icmremote* should be set to true in the cmbicmsrvs.ini file. Also be sure icmhostname, icmport, icmremotedb, icmnodename, and icmostype contain valid values.

Once the database is cataloged on the client machine, you should validate the connection by going to a DB2 Command Window and running **db2 connect to icmnlsdb user icmconct using password**. By default, icmconct is the database connection user ID to be used by clients. The user ID and password are stored, in encrypted format in cmbicmenv.ini. This file can be updated from the System Administrator Client, by selecting **Tools | Change Database ID/password** from the menu bar.

Any errors that occur while using the Windows Client will be logged in the log file directory. To determine what the log file directory is, select **Options | Preferences** from the menu bar, (see Figure 15–9).



☑ Display Welcome screen after logon

□ Automatically display Notelog when documents are opened

☑ Annotations are visible while being moved

☑ Immediately display changes made in annotation property dialogs to the selected annotations

Document viewer window: Default Behavior

Thumbnail bar options

○ Show thumbnail bar
● Hide thumbnail bar
○ Thumbnail bar visible only when thumbnails present

Thumbnail size: Small

Position: Bottom

Print options

Folder Print Recursions: 10

Scan options

Pages in first part: 5

All additional parts: 15

Log file directory: C:\Documents and Settings\Bryan Daniel\Application Data\IBM\Content Manager\LOG

Figure 15–9 *Windows Client Log File Directory*

The error log file is named **ICMClient.err**, and contains detailed error messages which are useful for troubleshooting. For example, when a document import fails, the following messages might be found in this file:

```
2002-10-17 11:04:47.939 [2852] viitem  :  Exception DKXDOError (-1) in
DKDDO::add()

2002-10-17 11:04:47.949 [2852] viitem  :  Error State:

2002-10-17 11:04:47.949 [2852] viitem  :  Error text: ICM9804: The security
token supplied with order store was invalid.::HTTP / 1.1 204 No Content
(SERVER RC) : 9804

2002-10-17 11:04:47.959 [2852] viitem  :  Filename: DKLobICM.cpp Function:
LineNumber: 2449

2002-10-17 11:04:47.969 [2852] viitem  :  Filename:
PExtractCommonDocStructICM.cpp Function:  LineNumber: 208

2002-10-17 11:04:47.969 [2852] viitem  :  Exception Class Name: DKXDOError

2002-10-17 11:04:47.979 [2852]: viitem  :2771: Exception thrown DKDDO::add().
Could not create an item.  Exiting..

2002-10-17 11:04:47.979 [2852]: importdl: 703: Error adding to server.
```

The important text is in bold. An explanation and action plan for the ICM9804 message can be found in the Content Manager publication entitled *Messages and Codes (SC27-1349-00)*. This particular error can be resolved by going to the library server configuration and choosing to regenerate the encryption key. (Be sure the resource manager server is running when you regenerate the encryption key.)

In the Windows Client log file directory, you will also find a file named **ICMClientLog.ini**. This file allows you to enable or disable tracing for different client components. For example, if you are experiencing problems with the login dialog, you can update the value for LOGINDLG from ***d*** to ***e***. Trace messages are logged to the **ICMClient.log** file.

Content Manager eClient

Like the resource manager, the Content Manager eClient is installed as a web application in WebSphere Application Server. However, when using WebSphere AEs, the eClient is not installed into the default server configuration (server-cfg.xml). Instead, the eClient installation program deploys the eClient web application into a new configuration file named IDM_ICM.xml. This file is located, by default, in C:\Program Files\IBM\Cmgmt. If the eClient installation program detects that the resource manager web application has been deployed into the default server configuration, it will redeploy the resource manager into the IDM_ICM.xml configuration file.

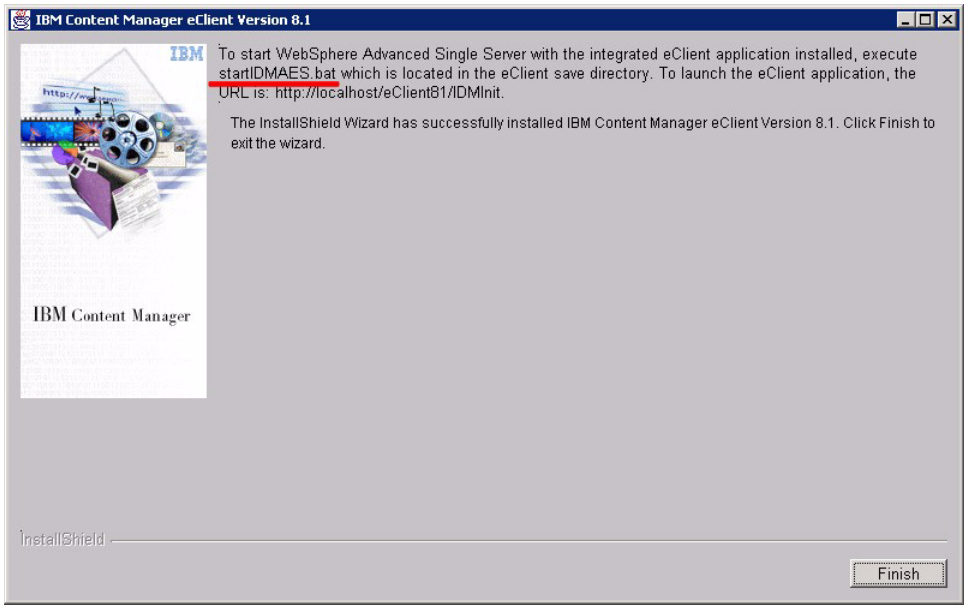
Note: When using WebSphere Application Server AEs, the eClient installation program will NOT deploy the eClient web application into the default server configuration.

When you select **Start** | **Programs** | **IBM WebSphere** | **Application Server V4.0 AES** | **Start Application Server**, the file named startServer.bat is run. This batch file starts the application server instance using the default configuration file:

\WebSphere\AppServer\config\server-cfg.xml.

Unfortunately, this configuration only contains the resource manager web application.

On the last window of the eClient installation, you may have noticed a message indicating how to start the eClient, (see Figure 15–10).


IBM Content Manager eClient Version 8.1

To start WebSphere Advanced Single Server with the integrated eClient application installed, execute startIDMAES.bat which is located in the eClient save directory. To launch the eClient application, the URL is: http://localhost/eClient81/IDMInit.

The InstallShield Wizard has successfully installed IBM Content Manager eClient Version 8.1. Click Finish to exit the wizard.

Figure 15–10 *eClient Installation Complete Window*

Note: To start the eClient web application, run C:\Program Files\CMeClient\startIDMAES.bat.

In order to start an application server instance using the eClient configuration file IDM_ICM.xml, you must run C:\Program Files\CMeClient\startIDMAES.bat. This batch file executes the following command:

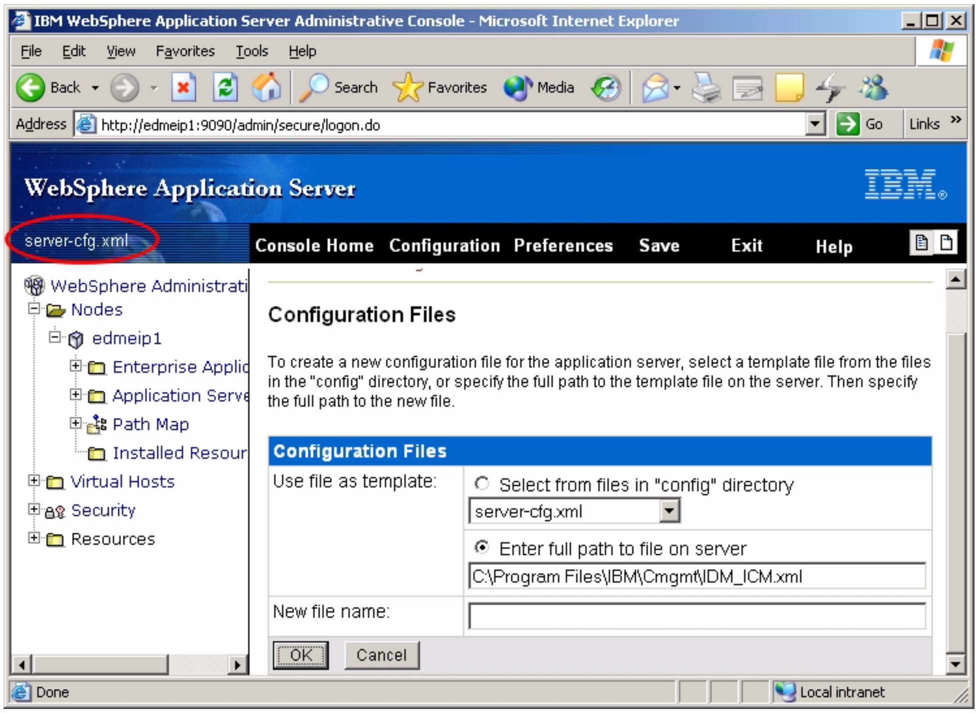
```
startserver -configFile "C:\Program Files\IBM\Cmgmt\IDM_ICM.xml" -serverName
"ICM_Server"
```

Notice that the application server instance is started using the custom configuration file. This configuration file contains the eClient and resource manager web applications.

8.1 **Note:** Run C:\Program Files\CMeClient\Save\idmwas.bat to automatically redeploy the eClient to the IDM_ICM.xml configuration file.

If you prefer to have the eClient web application in the default configuration file server-cfg.xml, you must manually deploy the eClient. Instructions for manually deploying the eClient can be found in the publication entitled *Installing, Configuring, and Managing the eClient Version 8.1 (SC27-1350)*.

To be sure the eClient web application is running, go to the WebSphere Administrative Console by selecting **Start** | **Programs** | **IBM WebSphere** | **Application Server V4.0 AES** | **Administrator's Console**. After you log on, the window shown in Figure 15–11 will appear.


IBM WebSphere Application Server Administrative Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
WebSphere Application Server
IBM
Console Home Configuration Preferences Save Exit Help
WebSphere Administrati
Nodes
edmeip1
Enterprise Applic
Application Serve
Path Map
Installed Resour
Virtual Hosts
Security
Resources
OK Cancel
Done
Local intranet

Address: http://edmeip1:9090/admin/secure/logon.do

server-cfg.xml

Configuration Files

To create a new configuration file for the application server, select a template file from the files in the "config" directory, or specify the full path to the template file on the server. Then specify the full path to the new file.

Configuration Files

Use file as template:
○ Select from files in "config" directory: server-cfg.xml
● Enter full path to file on server: C:\Program Files\IBM\Cmgmt\IDM_ICM.xml

New file name:

Figure 15–11 *Select eClient Configuration in WAS Administrative Console*

Look closely at the top left corner. Notice that you are working with the default configuration file named server-cfg.xml. In order to be able to work with the eClient web application, you need to open the IDM_ICM.xml configuration file. To do this, select the Configuration link at the top of the screen. Choose to open C:\Program Files\IBM\CMgmt\IDM_ICM.xml and select **OK**. The top left corner should now show the eClient configuration file. You may now expand Enterprise Applications and check to be sure the application named *IBM eClient 81* is running.

If you are unable to use *http://<hostname>/eClient81/IDMInit* to access the eClient, you should check the WebSphere Application Server standard out and standard error log files. These files are located, by default, in C:\WebSphere\AppServer\logs and are named **ICM_stdout.log** and **ICM_stderr.log** respectively. Problems with the eClient deployment (i.e. invalid classpath) will be logged in these log files.

The eClient configuration file, IDM.properties, allows you to adjust the eClient tracing. The two parameters that are used when troubleshooting, and their default values, are shown below. The valid values for TraceLevel are shown in Table 15–5.

```
TraceLevel = 1
WorkingDir=C:\\Program Files\\CMeClient\\logs\\
```

Table 15–5 *eClient TraceLevel Values*

TraceLevel	Description
0	tracing off
1	exceptions and errors
2	level 1 with the addition of general information, method entry, and method exit points
3	level 2 with the addition of API calls
4	level 3 with the addition of EIP non-visual bean Tracing
5	performance tracing

After updating the tracelevel value, you must restart the eClient web application. This can be accomplished by running stopIDMAES.bat followed by startIDMAES.bat.

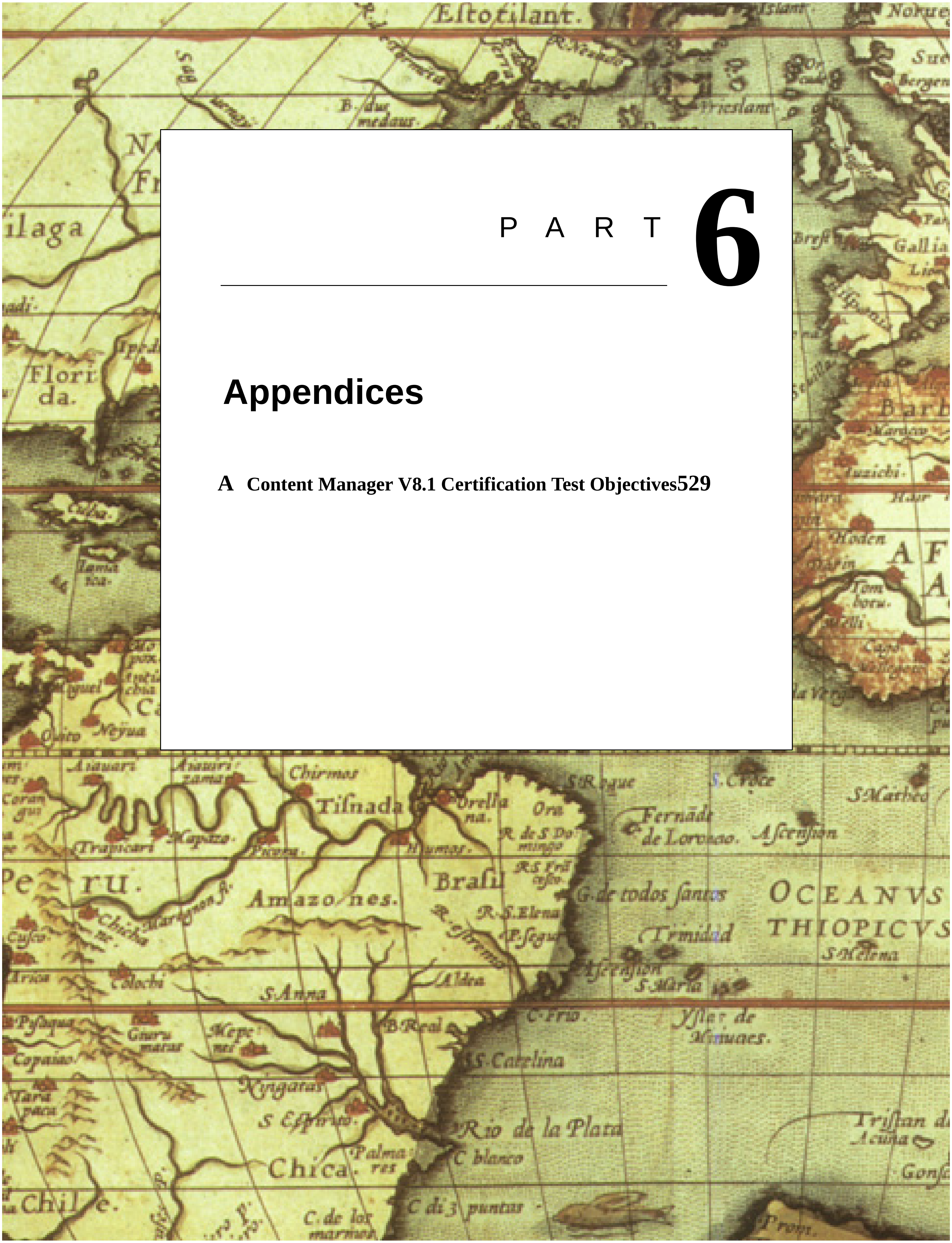
Summary

In this chapter, you learned how to troubleshoot problems in a Content Manager system. You saw that a typical Content Manager system includes more than a library server and resource manager component. Instead, when troubleshooting, you must be aware that components such as DB2 UDB, DB2 Text Information Extender, WebSphere Application Server, and IBM HTTP Server are all involved. Errors that occur in any one of the underlying software components may cause client functions to fail. As an administrator, you must determine which component is causing the error, why the error is being thrown, and how to resolve the error.

You also learned that the library server default log filename is ICMSERVER.LOG. The level of tracing and the location of this log file can be configured from the library server configuration. Higher levels of logging must can be achieved by manually updating the TRACELEVEL value in the ICMSTSYSCONTROL library server table.

When troubleshooting the resource manager, the IBM HTTP Server and WebSphere Application Server log files are useful in validating the deployment and configuration of the resource manager. When problems do arise, you should verify the database was created successfully and that the web application makes three database connections when started. The resource manager logs messages in a file named icmrm.logfile, and also contains a tracing facility that allows you to trace the different components of the resource manager.

The Content Manager Windows Client and eClient contain their own logging and tracing facility. The Windows Client log file directory can be determined by selecting **Options | Preferences** from the menu bar. Tracing various components of the Windows Client is controlled by a file named ICMClientLog.ini. When troubleshooting the eClient, you must rely on the standard out (ICM_stdout.log) and standard error (ICM_stderr.log) log files. Problems with the eClient can be traced by adjusting the tracelevel parameter in the IDM.properties file.



PART 6

Appendices

APPENDIX A

Content Manager V8.1 Certification Test Objectives

The IBM Content Manager Version 8 certification test requires that you have knowledge of the concepts of IBM Content Manager Version 8, its components and functions. Below is a list of the primary objectives for Test 442, IBM Content Manager Version 8. These objectives are listed here to assist you in your preparation for the exam, which you must pass to receive the IBM Certified Solutions Expert - IBM Content Manager Version 8.

As an IBM Certified Solutions Expert - IBM Content Manager Version 8, you should has detailed technical knowledge about IBM Content Manager Version 8. The certification candidate will be required to apply the concepts and have general knowledge about the IBM Content Manager portfolio. This specialist performs the following tasks related to IBM Content Manager Version 8: High-level design and requirements gathering; installation and configuration; troubleshooting; user and system administration; maintenance and performance tuning; and solution migration and integration.

This expert understands when IBM Content Manager Version 8 is the appropriate solution, and had the core competencies in installing, managing and installing Content Manager Version 8. This specialist has the knowledge of functions specific to the Content Manager Library Server, Resource Manager, System Administration, System Managed Storage, MS Windows client and Content Manager eClient.

This test contains a total of 64 questions. To pass this test you must score 64% or greater. You will have 90 minutes to complete this test. Detailed information on the IBM Professional Certification program including the IBM Content Manager Version 8 certification exam can be found at: http://www.ibm.com/certify.

I. High Level Design and Requirements Gathering

A. Design High Level Data Model

- Types of objects to be stored
- Size of objects
- Information attributes (metadata)
- References
- Links
- Child components
- Item types

B. Data Management

- Scalability (volume and size of stored objects)
- Retention requirements (where and for how long)
- Replication
- Data capture

C. System Design

- Number of users supported
- Number of servers
- Configuration topology (cities, time zones)
- System Managed Storage
- Security (e.g. fire walls, single sign on)
- Line of Business integration

D. Document Routing / Workflow

- Define workflow process
- Identify task list and nodes

II. Installation / Configuration

A. Verify prerequisites (WebSphere, DB2)

B. Verify co-requisites (Tivoli Storage Manager)

C. Verify successful installation

III - Troubleshooting

A. Run traces to diagnose problem

B. Review error messages to determine problems

- Application logs / System Log
- DB2 tables / Oracle logs
- Operating System logs / Event Logs
- Network logs
- WebSphere
- Tivoli Storage Manager

C. Check configuration (INI & CFG Files)

IV. System Administration

A. Data Modeling

- Define attributes, item types, child components

B. Define document routing process

C. User Administration

- Manage user roles and user groups
- Set access listing controls / privileges
- Set user system parameters (e.g., log out time)
- Define LDAP considerations

D. Customize server platforms and options

V. System Managed Storage

A. Define storage hierarchies and define devices (Tape, CDRom, Optical)

B. Define archival rules / schedules

C. Identify Tivoli Storage Manager relationships

VI. Maintenance and Performance Tuning

A. Evaluate performance against criteria

- Timing (batch loads/retrieves, Image Loads, User response, Maximum
- Loads)
- System Resources (File size, CPU usage, Memory usage, DASD usage, Network traffic)

B. Optimize server performance

C. Backup and restore

VII. Content Manager Clients

A. Perform Queries/Searches

- Parametric Queries
- Text Queries
- Combine Queries (Parametric / Text)

B. Create, retrieve, update and delete

VIII. Solution Migration

A. Migrate from previous versions

- Library servers
- Object servers

B. Migrate to larger systems or different platforms

IX. Solution Integration

A. User exits, Client OLE interfaces, Toolkit

X. Core Product Information

A. Ability to define products (CM, OD, EIP)

B. Identify appropriate product to resolve specific customer problems

C. Product functions and features

Sample Questions

1. Auto-foldering is implemented by which of the following?

A. Reference

B. Child component

C. Link

D. Foreign key

2. A Content Manager foreign key is primarily used to

A. Limit the value a user can enter for an attribute

B. Limit the item types a user can select for loading information

C. Select a different language to represent the attribute entry

D. Auto link item types together.

3. A business will be implementing Content Manager on a single system, but would like to off-load the responsibility of managing users from the Information Technology department to the different departments. Which of the following must the System Administrator do in order to give each department responsibility for their users, without jeopardizing the security of the overall system?

A. Set up Access Control Lists for each area, allowing the area administrator to create users and assign their access control list.

B. Set up administrative domains giving each area responsibility for a domain of users.

C. Set up the Content Manager system with each area having an assigned Library and Resource Manager database.

D. Segment the Content Manager implementation into virtual system views assigning each area their restricted system view.

4. A chemical company will use Content Manager to track government standards compliance verifications to demonstrate that all employees have been certified on the new standards. This requires that the process wait until a number of documents are ready to be processed. Which of the following should be done in implementing Content Manager?

A. Use document routing with a workbasket and resume list.

B. Use document routing with a collection point and resume list.

C. Use document routing with a workbasket and overload limits.

D. Use document routing and collection overload limits.

5. An administrator installed a Content Manager Server on Machine A and now wants to install the System Administration Client on Machine B. Which of the following software components must be on Machine B?

A. DB2 Application Development Client

B. Microsoft Visual C++ Compiler

C. DB2 Text Information Extender

D. DB2 Runtime Client

6. How can an administrator verify which TSM client option file is being used by the resource manager?

A. Run the TSM Backup Archive Client

B. Use the System Administration client to view the resource manager properties

C. Check the DSMI_CONFIG variable in the icmrm.properties file

D. Check the ICMSERVER.LOG file

7. Which file should an administrator inspect to determine if the resource manager database was created successfully?

A. icmserver.log

B. icmrm.logfile

C. rmconfig.log

D. icmcrrmdb.log

8. Which of the following tests does NOT indicate if the Secured Sockets Layer (SSL) is configured correctly?

A. A new resource manager collection can be created from the System Administration Client

B. The URL https://<hostname>/icmrm/ICMRMResourceManager is accessible

C. A document can be successfully imported into the resource manager

D. The URL https://<hostname>/icmrm/snoop is accessible

9. What is the minimum trace level required to see which stored procedures are

getting executed by the Library Server?

A. Basic Trace

B. Data Trace

C. Detailed Trace

D. Performance Trace

10. A company is migrating from Content Manager version 7.1 to 8.1. While importing metadata into resource manager, the following error is received:

DB21061E Command line environment not initialized.
Error opening objtextparts.del
loading demgr table
Error in loading devmgr table. Please check .\devmgrload.log for more information

Which of the following could be the cause of this problem?

A. Userid which is used to run the migration utility does not have the necessary database privileges.

B. The utility was not run from a DB2 Command Window

C. The system is out of storage space

D. Resource manager is not running

11. The Content Manager eClient is used to perform a query. The search results is displayed, but none of the documents can be opened. What could be the cause of the problem?

A. Library server is not running

B. The documents contain more than one part

C. Resource Manager web application is not running

D. SSL is not configured properly

12. An administrator has used the System Administration client to update the password for the database connection userid (icmconct). Which of the following files will contain this updated information?

A. cmbicmenv.ini

B. cmbicmsrvs.ini

C. cmbcmenv.properties

D. cmbclient.ini

13. Which of the following item type classifications will NOT allow text searches to be performed on the content of a text document?

A. Document

B. Item

C. Document Part

D. Resource Item

14. Which of the following is NOT required to define a collection point work node?

A. A folder item type

B. Priority

C. A required item type

D. Quantity of item

15. When a system administrator defines a new user, what the default value is she not able to assign to this new userID?

A. A default library server

B. A default resource manager

C. A default collection

D. A default item access control list

16. 16.A Healthcare provider wants to achieve the following scenario:

Two users (A and B) logon to the Content Manager system and perform searches across all the item types in the system. Users A receives information from the "Medical" item type and the "Accounting" item type while user B only receives information back from the "Medical" item type.

The Content Manager system is set as library ACL (access control lists) binding. The library ACL name is "myCompanyACL".

I. Assign proper privilege set to each user.

II. Assign proper privilege set to the user group(s) associated with each user.

III. Configure "myCompanyACL’ properly.

IV. assign different ACL to item type "Medical" and "Accounting".

In which of the above ways, if any, can this be achieved in the Content Manager system?

A. I and III

B. I and IV

C. II and III

D. II and IV

17. Before creating a new Content Manager user "newuser", what does a system administrator have to do?

I. Create a system user "newuser" on the workstation.

II. Create a database user "newuser" in the library server database.

III. Create a database user "newuser" in the resource manager database.

Choose all valid option(s) from the above.

A. I and II

B. I and III

C. I, II and III

D. None

18. Which of the following LDAP servers is not supported by Content Manager?

A. IBM Directory Server

B. Novell Directory Services

C. Microsoft Active Directory of Windows 2000

D. Lotus Domino Directory Notes Address Book

19. A system administrator wants to configure a Content Manager library server to handle 50 concurrent connections. How does he implement it?

A. Make the change in the System Administration Client.

B. Make the change in the Content Manager configuration file.

C. Make the change in DB2 configuration.

D. Nothing because Content Manager handles it internally.

20. Which device manager is used to communicate with a Tivoli Storage Manager server?

A. ICMFILEPATH

B. ICMHDDM

C. ICMADDM

D. ICMVCDM

21. A Content Manager administrator wants to manually start the migrator process, but first wants to know how many documents are candidates for migration. What table column can be queried to determine this information?

A. ACTIONDATE column in the SBTITEMS table

B. ITEMID column in the ICMPARTS tables

C. OBJ_ACTIONDATE column in the RMOBJECTS table

D. MIGDATE column in the RMITEMS table

22. When integrating a resource manager server with Tivoli Storage Manager, what TSM information must the Content Manager administrator know?

I. Nodename and password
II. Management class name
III. Storage Pool name

A. I and II

B. I and III

C. II and III

D. I, II, and III

23. For better performance, a System Administrator wants to remove the midtier image conversion in the Content Manager eClient. Where should the change be made to implement this?

A. IDMadminDefaults.properties and IDM.properties

B. cmbclient.ini and cmbcs.ini

C. IDM.properties and icmcmbenv.ini

D. IDMadminDefaults.properties and cmbclient.ini

24. After loading a significant number of large documents into Content Manager, the amount of time needed to perform a query has increased noticeable. Which of the following actions would most likely improve the search performance?

A. Move the larger documents to a faster storage device

B. Reorganize the resource manager database

C. Create indexes on the frequently used library server database tables

D. Migrate documents to Tivoli Storage Manager

25. When peforming a full backup of the Content Manager system, which of the following can be safely excluded?

A. Library server database

B. Resource manager database

C. Files in the "staging" directory

D. Files in the "lbosdata" directory

26. A Content Manager user is searching for documents by using the basic search functionality of the Windows Client. Which of the following can the user search for?

I. Documents
II. Folders
III. Links
IV. Worklists

A. I and II

B. I, II, and III

C. I, II, and IV

D. I, II, III, and IV

27. After installing the Content Manager eClient, what file must be updated to allow users to import documents?

A. IDMinstall.properties

B. IDMenv.ini

C. IDMadminDefaults.properties

D. IDM.properties

28. A company plans to migrate their Content Manager system from version 7.1 to 8.1. Which of the following actions is NOT required before running the migration wizard?

A. Backup library server and object server databases

B. Have all users logout from the system

C. Complete the destager process

D. Stop the database manager

29. When using the Windows Client, what user exit can be called when a document is moved to a new item type?

A. Search

B. Sort

C. Resource manager storage

D. Import

30. A company wants to leverage their Content Manager system by archiving attachments that currently exists on their Lotus Notes mail servers. Which of the following products would easily allow them to do this?

A. Enterprise Information Portal

B. Content Manager OnDemand

C. Tivoli Storage Manager

D. Content Manager CommonStore

Answers to Sample Questions

Item Number	Content Code	Key	Rational
1	1A	C	Auto foldering is implemented via directional links, and can be configured in the Administration Client.
2	1B	A	A Content Manager foreign key is primarily used to limit the value which a user can enter for an attribute.
3	1C	B	Content Manager allows administrative domain administrator to maintain users in its domain. The domain administrator does not have any authority in other domain.
4	1D	B	Folders in collection point collect required number of documents before they move to the next step in the process.
5	2A	D	The System Administration Client requires the DB2 Application Development Client in order to access the library server database.
6	2B	C	The client option file used by the TSM Client APIs is specified by the DSMI_CONFIG variable. This variable is defined in the resource manager icmrm.properties file.
7	2C	D	icmcrrmdb.log is the resource manager database creation log file
8	2C	C	Content Manager does not require SSL to import a document into the Resource Manager successfully.
9	3A	A	Basic Trace is the minimum trace level required to see which stored procedures are getting executed by the Library Server.

Item Number	Content Code	Key	Rational
10	3B	B	Content Manager migration import utilities must be executed in DB2 Command Window.
11	3B	C	In order to import or retrieve objects from Content Manager, the Resource Manager web application (icmrm) must be running.
12	3C	A	cmbicmenv.ini contains the database connection userid and password in encrypted format. The information in this file can be updated from the System Administration client.
13	4A	B	An item type that is classified as "Item" only contains metadata and does not contain any object parts. Therefor, although you can perform a text search on the attributes, there is not part to perform a text search on.
14	4B	B	While defining a collection point work node, you must provide a folder item type, a required item type and quantity of item.
15	4C1	A	When creating a new user, you may define the default resource manager, a default collection and a deafult item access control list. Since there is only one library server in the system, you do not need to assign a default value.
16	4C2	A	Since the Content Manager system is setup for library ACL (access control lists) binding, ACL "myCompanyACL" is used when everyone retrieve items from any item type. So, it must be configured properly. Also, proper privilege set has to be assigned to each user.
17	4C3	D	No pre-requirement to create a new Content Manager user.

Item Number	Content Code	Key	Rational
18	4C4	B	Content Manager supports IBM Directory Server, Microsoft Active Directory of Windows 2000 and Lotus Domino Directory Notes Address Book.
19	4D	C	Since a Content Manager library server is basically a database, you need to make the change in DB2 configuration.
20	5A	A	ICMADDM is the TSM device manager
21	5B	C	The migrator will inspect any document which has an actiondate less than or equal to the current system date.
22	5C	A	The nodename and password to be used to connect to TSM must be known. The TSM volume name must match the management class name. Storage pool information is not needed to integrate CM with TSM.
23	6A	A	The applet viewer can retrieve documents directly from the resource manager and perform client side conversions. You enable the applet viewer in IDM.properties, and set the mime type which will use the applet viewer in the IDMadminDefaults.properties.
24	6B	C	Searches are performed by the library server and have nothing to do with the resource manager or the size of the documents. Creating database indexes usually improves the query performance.
25	6C	C	"Staging" directory is used as a cache for documents stored within TSM. This directory contains a temporary copy of the original documents.

Item Number	Content Code	Key	Rational
26	7A	A	The Windows Client allows users to search for documents and folders. You can also specify document routing status, process, and step. However, you canÕt specify a worklist or a link.
27	7B	D	To allow the import functionality, the importSupported parameter in the IDM.properties file must be set to true.
28	8A	D	While migrating Content Manager system from version 7.1 to 8.1, the database manager must be running.
29	9A	C	The resource manager storage (also called Change SMS) user exit is called whenever the item type is changed for an item.
30	10A	D	CommonStore for Lotus Domino allows businesses to archive emails and attachments into Content Manager.

Index