IBM Content Manager for Multiplatforms

Planning and Installing Your Content Management System

Version 8 Release 2

GC27-1332-01

IBM Content Manager for Multiplatforms

Planning and Installing Your Content Management System

Version 8 Release 2

GC27-1332-01

Note

Before using this information and the product it supports, read the information in "Notices" on page 543.

Second Edition (March 2003)

This edition applies to Version 8 Release 2 of IBM Content Manager for Multiplatforms (product number 5724-B19) and Version 8 Release 2 of IBM Enterprise Information Portal for Multiplatforms (product number 5724-B43) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this guide

This guide provides the information that you need to plan for, install, and configure Content Manager components on the following operating systems:

- Microsoft® Windows®
- AIX®
- Sun Solaris Operating Environment (hereinafter referred to as Solaris)

The guide provides installation guidelines and recommendations as well as steps for each installation task.

Very Important - Two key parts of the IBM® Content Manager for Multiplatforms package are:

1. The ″Start Here″ CD
2. This *Planning and Installing Your Content Management System* guide

Follow these steps for a smooth installation experience:

Step 1.

Familiarize yourself with Content Manager and get an overview of the product by looking over the following sections of *Planning and Installing Your Content Management System*:

- Chapter 1, “Introducing Content Manager”, on page 3
- Chapter 3, “Planning for Content Manager”, on page 23
- Chapter 6, “Content Manager hardware and software requirements” , on page 55

Note: Don’t try to install any of the products until you have used the ″Start Here″ CD in step 2.

Step 2.

Insert the ″Start Here″ CD into the CD drive of any of your workstations. The CD launches automatically and:

- Explains the contents of the Content Management package
- Informs you of the product capabilities
- Explains potential system configurations
- Assists you with product requirements, planning information, and installation steps
- Points (or links) to important information in this guide (as you need it) during the planning process.
- Provides printable planning charts as a result of decisions that you make during the planning process.

Step 3.

Intall the products in the order indicated by the Output Planning charts from the ″Start Here″ CD.

Use this guide, along with your output charts, to step you through the installation of the various prerequisite programs and Content Managent components. This guide is divided into five parts as follows:

- Part 1 addresses the planning aspects of Content Manager
- Part 2 leads you through an entire installation for the Windows operating system
- Part 3 leads you through an entire installation for the AIX operating system
- Part 4 leads you through an entire installation for the Sun Solaris operating system
- Part 5 guides you through any after-install program installation and configuration procedures, including the uninstall procedures.

Who should use this guide

Use this guide if you need to plan for, install, configure, upgrade, or migrate the Content Manager system for your enterprise. Application programmers who want to create client applications might also want to read this guide.

Skills that are required

Depending on the configuration of your Content Manager system, you should be familiar with one or more of the following operating systems: Windows, AIX, and Sun Solaris.

To design and install a custom system, you need to be familiar with the following:

- One of the following communications protocols:
  - Transmission Control Protocol/Internet Protocol (TCP/IP)
  - System Network Architecture (SNA), Advanced Peer-to-Peer Communication (APPC), or Advanced Peer-to-Peer Networking® (APPN)
- System operation and network administration
- Database administration on DATABASE 2 (DB2®) or Oracle

Where to find more information

Your product package includes a complete set of information to help you plan for, install, administer, and use your system. Product documentation and support are also available on the Web.

Information included in your product package

The product package contains an information center and each publication in portable document format (.PDF).

The information center

The product package contains an information center that you can install when you install the product. For information about installing the information center see *Planning and Installing Your Content Management System*.

The information center includes the documentation for Content Manager, Enterprise Information Portal, and IBM Content Manager VideoCharger. Topic-based information is organized by product and by task (for example, Administration). In addition to the provided navigation mechanism and indexes, a search facility also aids retrievability.

PDF publications

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

Table 1 shows the Content Manager publications included with IBM Content Manager for Multiplatforms.

Table 1. Content Manager publications

File name	Title	Publication number
install	*Planning and Installing Your Content Management System*[1]	GC27-1332-01
migrate	*Migrating to Content Manager Version 8*	SC27-1343-01
sysadmin	*System Administration Guide*	SC27-1335-01

When you order IBM Content Manager for Multiplatforms, you also receive IBM Enterprise Information Portal for Multiplatforms. Or, you can separately order IBM Enterprise Information Portal for Multiplatforms. Table 2 shows the Enterprise Information Portal publications that are included with the product.

Table 2. Enterprise Information Portal publications

File name	Title	Publication number
apgwork	*Workstation Application Programming Guide*[1]	SC27-1347-01
ecliinst	*Installing, Configuring, and Managing the eClient*	SC27-1350-02
eipinst	*Planning and Installing Information Integrator for Content*	GC27-1345-01
eipmanag	*Managing Information Integrator for Content*	SC27-1346-01

Table 2. Enterprise Information Portal publications (continued)

File name	Title	Publication number
messcode	*Messages and Codes*[2]	SC27-1349-01

Notes:

1. The *Workstation Application Programming Guide* contains information about programming applications for both Content Manager and Enterprise Information Portal.
2. *Messages and Codes* contains the messages and codes for Content Manager and Enterprise Information Portal.

Support available on the Web

Product support is available on the Web. Click **Support** from the product Web sites at:

www.ibm.com/software/data/cm/

www.ibm.com/software/data/eip/

The documentation is included in softcopy with the product. To access product documentation on the Web, click **Library** on the product Web site.

An HTML-based documentation interface, called Enterprise Documentation Online (EDO), is also available from the Web. It currently contains the API reference information. Go to the Enterprise Information Portal Library Web page for information about accessing EDO.

How to send your comments

Your feedback helps IBM to provide quality information. Please send any comments that you have about this publication or other Content Manager or Enterprise Information Portal documentation. You can use either of the following methods to provide comments:

- Send your comments from the Web. Visit the IBM Data Management Online Reader’s Comment Form (RCF) page at:

  www.ibm.com/software/data/rcf

  You can use the page to enter and send comments.
- Send your comments by e-mail to comments@vnet.ibm.com. Be sure to include the name of the product, the version number of the product, and the name and part number of the book (if applicable). If you are commenting on specific text, include the location of the text (for example, a chapter and section title, a table number, a page number, or a help topic title).

What’s new in Version 8.2?

Version 8.2: Version 8.2 includes a variety of enhancements from Version 8.1. Version 8.2 adds more workflow features to the eClient, increases resource management function, and supports the latest in database and client technology, including DB2 Universal Database Version 8.1, Oracle Version 8.1.7.4 and Version 9.2.0.1, and WebSphere Version 5. These highlights, and other enhancements to the Version 8.2 product, are summarized below:

Enterprise Information Portal name change to IBM Information Integrator for Content

Enterprise Information Portal has been renamed to Information Integrator for Content. Although the names of the books have changed for Version 8.2, the text within the books continues to show the product name Enterprise Information Portal. When searching the Web for more information, you can continue to use Enterprise Information Portal, or EIP, until the transition to the new name is complete.

Support for Oracle Version 8.1.7.4 or Version 9.2.0.1 or later

Content Manager V8.2 adds support for Oracle databases managing the metadata stored in both library server and resource manager. Migration tools are included for Oracle users of Content Manager Version 7. **Note:** Oracle does not manage Enterprise Information Portal database server contents.

Replication

Content Manager V8.2 includes resource manager replication, which is the ability to store objects in multiple locations, managed by replication resource managers. Object replicas will behave as LAN cache objects for improved load balancing.

LAN cache

LAN cache support in Content Manager V8.2 provides application-transparent caching, using local servers as defined by the system administrator.

Support for DB2 UDB V8.1

Content Manager V8.2 and Enterprise Information Portal V8.2 supports DB2/UDB V8.1. The connection concentration feature of DB2 V8.1 provides increased scalability for two-tier applications and clients (such as the Content Manager V8 Client for Windows). DB2/UDB V8.1 has replaced the DB2 Universal Database Text Information Extender (TIE) with Net Search Extender (NSE).

Support for WebSphere Application Server Version 4 and Version 5
WebSphere Application Server Version 5 introduces server deployment and data access and management from any web browser.

Federated folders
eClient now has the ability to organize documents and native folders from multiple repositories into a single federated folder and start that folder on a workflow. Federated folders also allows users to persistently store search results in the EIP federated database where users can retrieve them at any time. Full CRUD (create, retrieve, update, and delete) operations are available against these federated folders without re-indexing.

Advanced workflow collection points
Workflow is now fully supported on AIX and Solaris. The workflow builder, APIs, Collection Points Monitor, and JavaBeans provide improved workflow function and usability.

Microsoft Visual Studio .NET for building applications
The Content Manager and Enterprise Information Portal 8.1 and later APIs now support Microsoft Visual Studio .NET for writing content management applications or to integrate applications built using Microsoft Visual Studio .NET.

Version 8.1: Version 8.1 begins a legacy of integration and versatility. One of the many highlights and improvements from previous Content Manager products is the new data model structure which allows for more document customization. The changes to the Content Manager product in Version 8.1 are summarized below:

Improved performance
The library server and resource manager use DB2 stored procedures and leverage DB2 technology to significantly reduce network traffic and improve performance and scalability.

Support for Sun Solaris
Both the library server and resource manager can be installed on Sun Solaris.

Enhanced data model
The new hierarchical data model provides the basis for customized compound document management solutions.

Improved workflow
Through integrated document routing, workflow capabilities have been improved with sequential routing, dynamic routing, and collection points.

Integrated text search
In addition to attribute-based searching, client users can now perform full-text searching on text-based document information. The text search function now uses the DB2 Universal Database Text Information Extender, which contributes to a streamlined process for setting up text searching.

Common system administration
A single client application provides separate access to Content Manager and Enterprise Information Portal. Within Content Manager, administrative domains provide a way to limit administrative access to subsections of the library server.

Full-function desktop client and enhanced eClient
Client enhancements provide users with an out-of-the-box application for rapid deployment or line of business application integration. The Client for Windows supports integrated text search, document routing, the hierarchical data model (to a single child component level), versioning, and index during import. The eClient includes integrated text search, EIP advanced workflow, version control, and multi-valued attributes.

Easier installation
Installation is consistent across supported operating systems and customized installation information is provided by the Start Here CD's Planning Assistant. Silent and console installations are also provided.

Information center
The browser-based information center includes the documentation for Content Manager, Enterprise Information Portal, and IBM Content Manager VideoCharger. Topic-based information is organized by product and by task (for example, Administration). In addition to the provided navigation mechanism and indexes, a search facility also aids retrievability.

Accessibility
Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features for this product include:

- The ability to operate all features using the keyboard instead of the mouse.
- Support for enhanced display properties.
- Options for video and audio alert cues.
- Compatibility with assistive technologies
- Compatibility with operating system accessibility features

  - Accessible documentation formats

PeopleSoft and Siebel integrations
Users of PeopleSoft and Siebel applications can now configure these applications to access content stored in a variety of content servers using the eClient.

Part 1. Planning for Content Manager

This section contains information for planning your Content Manager system across all operating systems. It addresses the following topics:

- Chapter 1, “Introducing Content Manager”, on page 3
- Chapter 2, “Introducing the XYZ Insurance scenario”, on page 17
- Chapter 3, “Planning for Content Manager”, on page 23
- Chapter 4, “Introducing Enterprise Information Portal”, on page 37
- Chapter 5, “Planning your Enterprise Information Portal system”, on page 43
- Chapter 6, “Content Manager hardware and software requirements”, on page 55
- Chapter 7, “EIP hardware and software requirements”, on page 67

Chapter 1. Introducing Content Manager

In the past, business communication consisted of information on paper. Conversations were documented by taking notes on paper. Presentations were typed onto paper. Correspondence was sent to customers through the mail. A document was considered to be information on paper.

Today, a document is much more than information on paper. Business is conducted in many forms, some, unheard of just a few years ago. In today's world, business is complicated. Most businesses use multiple transactions, and many means of communicating, negotiating, or working with their customers. They use fax, e-mail, electronic presentations, and electronic meeting sessions, for example. All of these transactions are stored into some electronic medium and are considered to be documents, or at least the contents of a stored information unit that we call a document.

Most businesses need a way to manage the content of their documents. They need a way to capture each event or communication that occurs with their customers. They need to be able to store the content, organize it, and retrieve it in the blink of an eye. They need to look at it, update it, print it, e-mail it, fax it, or even throw it away when it is no longer needed.

It would be very difficult and expensive for some businesses to create their own program, or even to assemble a variety of programs, and try to get them to work together to solve their content management problem.

The Content Manager solution

Content Manager provides the solution.

Content Manager doesn't have a single process for solving the problem, instead, it has an unlimited variety of flexible ways to manage content. Content Manager provides components that work together to solve your business needs.

The Content Manager solution includes:

- Support for multiple operating systems
- A Java™-based tool for managing the system
- Client options
- Browser access
- Support for business documents of almost every kind

- Administration tools for defining users and user privileges
- Efficient methods for keeping the system secure
- Features for managing the flow of work through the system

Building a Content Manager system

This section shows how the Content Manager system fits together. Each component, feature, or a related program is described one at a time, then how it works with the rest of the system.

The library server component

The library server is the key component of the Content Manager system. It is called the library server because it performs the functions that a library catalog file in a real library performs. It is where you define the information that you store in your library.

The library server is the component of a Content Manager system that stores, manages, and provides access control for objects stored on one or more resource managers. The library server processes requests (like update or delete) from one or more clients and maintains data integrity between all of the components in the Content Manager system.

User access to objects stored on any resource manager in the system is directly controlled by the library server. A library server relies on a relational database management system (RDBMS), like DB2 Universal Database™, to manage the content and perform parametric searches, text searches, and combined (parametric and text) searches.

You can directly access the library server using SQL (Structured Query Language) or a relational database client.

A Content Manager system requires one library server, which can run on the Windows, AIX, or Solaris operating system. Figure 1 on page 5 shows the library server.

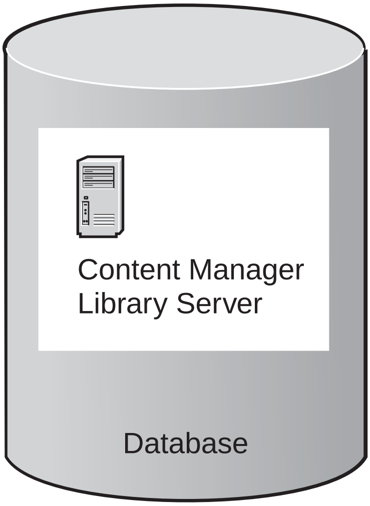

Figure 1. Library server

The following programs are provided in this package to work with the library server:

IBM DB2 Universal Database
The IBM DB2 Universal Database software provided in this package is required to run with the library server (and must be installed on the same machine as the library server).

Text Search feature
Content Manager includes an optional text search feature that allows for full text searching through documents in the Content Manager database. To use it, you must plan ahead and install the DB2 Text Information Extender (TIE) when you are installing the prerequisite DB2 software for the library server.

Document routing
Document routing (called ″workflow″ in previous versions of Content Manager) is an integrated part of the basic library server installation. It is provided to help you manage your ″work-in-process″ by creating processes and work nodes:

Process
A series of steps defined by an administrator through which a document is routed.

Work node
A step within a process.

Access to processes and work nodes is controlled by the system administrator through access control lists. More information is provided in the *System Administration Guide*.

The resource manager component

Add the resource manager to the system. It can be on the same work station as the library server, or it can be on its own computer (depending on what you want to do and how you want to configure your system). Figure 2 shows the resource manager and its relationship to the library server.

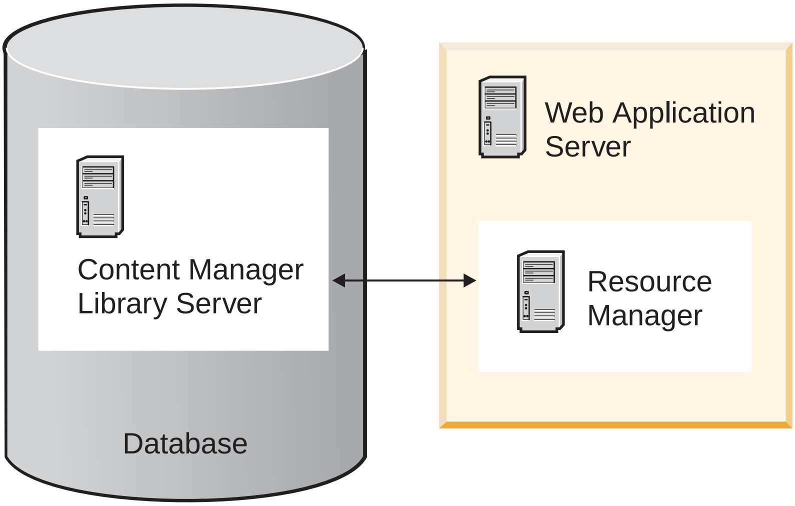

Figure 2. Resource manager

The resource manager efficiently and automatically stores objects for Content Manager. Users store and retrieve digital objects on the resource manager by routing requests through the library server. A single library server can support multiple resource managers and content can be stored on any of these resource managers.

Resource managers can be distributed across networks to provide convenient user access.

Using the Content Manager Client for Windows, you can communicate with the resource manager and perform simple functions like storing, retrieving or updating objects. You can also perform more complicated functions (that you can learn about later).

The following programs are provided in this package to work with the resource manager:

IBM DB2 Universal Database

The IBM DB2 Universal Database software provided in this package is required to run the resource manager. It can be installed on the same machine as the resource manager, or it can be installed on a separate machine. Depending on the speed and storage requirements of your Content Manager system, you could even have the library server and the resource manager share the same DB2 database that is installed on the library server machine.

WebSphere® Application Server (WAS)

The IBM WebSphere Application Server (WAS) software provided in this package is required to run with the resource manager and must be installed on the same machine as the resource manager.

The IBM WebSphere Application Server (WAS) provides an environment for open distributed computing. Users and processes on a wide variety of platforms can interact by using the facilities provided by WAS.

Tivoli® Storage Manager (TSM)

Tivoli Storage Manager (TSM) is provided so that you can optionally store long term objects on devices other than the fixed disks attached to the resource manager.

TSM is a client/server product that provides storage management and data access services in a heterogeneous environment. It supports various communication methods, provides administrative facilities to manage the backup and storage of files, and provides facilities for scheduling backup operations.

The system administration client component

You use the system administration client to oversee the entire Content Manager system. With the system administration client, you perform tasks like:

- Defining your data model
- Defining users and their access to the system
- Managing storage and storage objects in the system

These tasks are explained in detail in “Planning for system administration” on page 29. Figure 3 shows a system administration client connected to the system.

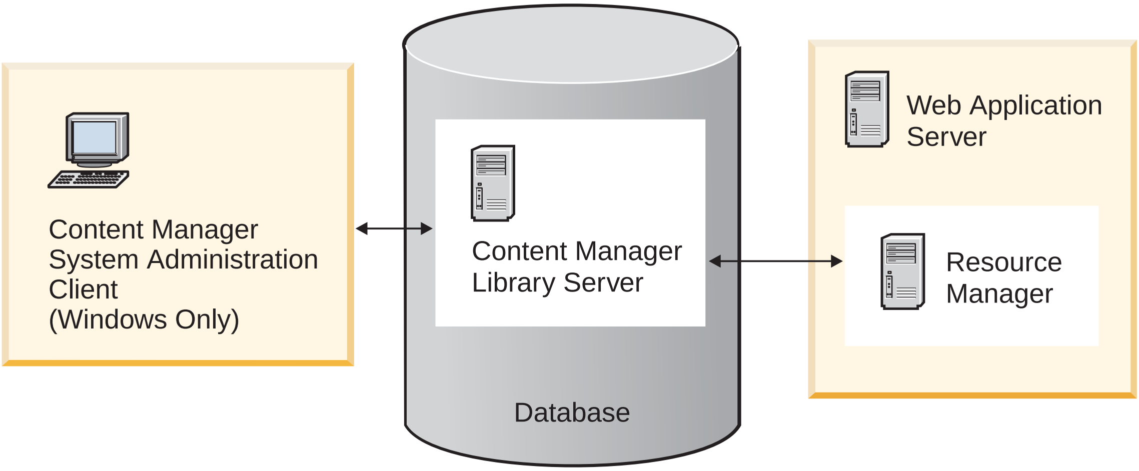

Figure 3. System administration client

The system administration client component can be installed on any of the workstations that other components are installed, or it can be on its own workstation.

LDAP option
During the Content Manager installation, you have the option to decide if you want to use LDAP (Lightweight Directory Access Protocol) with the Content Manager system. It allows you to define a directory to store a single user ID and password for each user with secure, controlled access to any or all components of the Content Manager system through a single sign-on (or logon). For more information, see “Planning for user management” on page 34.

Client options

There are many ways to customize the Content Manager system to fit the business needs of your enterprise. Your exact process depends on how your enterprise chooses to implement and configure the system. Figure 4 on page 9 shows a Client for Windows attached to the system.

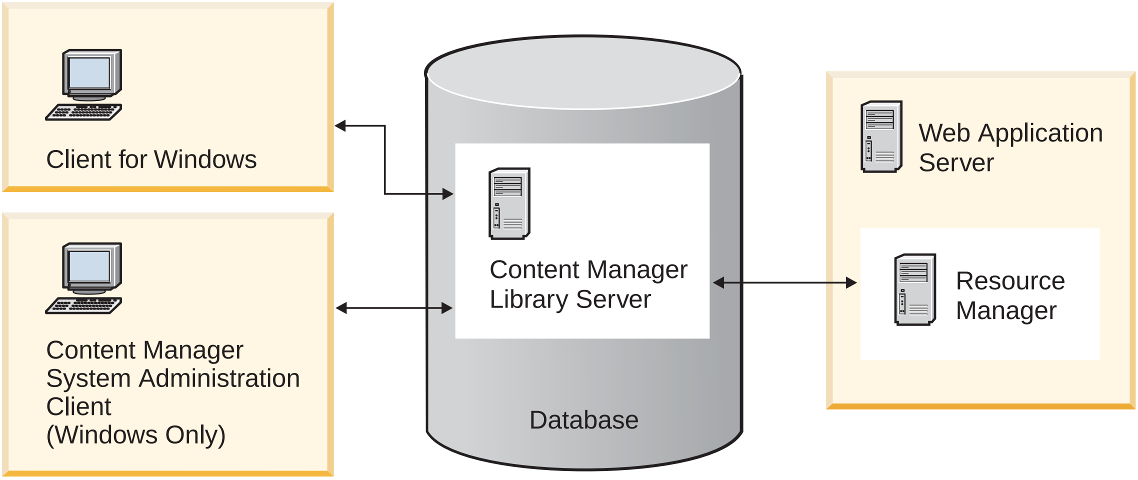
Client for Windows
Content Manager System Administration Client (Windows Only)
Content Manager Library Server
Database
Web Application Server
Resource Manager

Figure 4. Client for Windows

One of the options that you have is how you implement your client. Two options are available in this package: the Client for Windows, or the eClient. You may also decide to create your own client for your specific needs.

Client for Windows

The Client for Windows is installed on a Windows system. It provides an interface that enables you to import documents into the system, view them, work with them, store them, and retrieve them.

The Client for Windows can also be run in a Terminal Server Edition (TSE) environment. The number of users that can be supported on any one TSE server depends on the memory, processing power, and other factors on the server, as well as on the amount of activity for each client user. All client actions are supported in this environment, except for scanning (which must be done on a local machine).

eClient

The eClient can be installed on any system that has an Internet Explorer (Version 5.0 or higher) or a Netscape Navigator (Version 4.6 or higher) browser installed. This browser-based client allows users to connect, query, create, update, delete, and display documents and folders.

Creating your own client

You can create customized Content Manager applications by using client APIs and user exit routines that are part of the ICM connector that comes with Enterprise Information Portal. You can use these APIs to:

- Access information in the library server and resource manager
- Customize document processing
- Design your own data model

The IBM Enterprise Information Portal for Multiplatforms product

A subset of the Enterprise Information Portal (EIP) product is available in this package to provide search and retrieval capability across heterogeneous datastores, including:

- IBM Content Manager OnDemand
- IBM Content Manager for iSeries™
- Lotus® Domino™.Doc
- IBM DB2 Universal Database
- IBM ImagePlus® for OS/390®

If a required connector doesn’t exist it can easily be made. After it is made, that previously separate system can be searched in conjunction with all of its peers in one federated search. This gives you the ability to contextually provide access to all relevant data.

The IBM Content Manager VideoCharger for Multiplatforms product

The IBM Content Manager VideoCharger product is available as a separate product offering (not part of this package).

By installing the IBM Content Manager VideoCharger on a separate machine and connecting it to Content Manager through the resource manager, you can integrate video and audio files, (called *media objects* in Content Manager, and *assets* in IBM Content Manager VideoCharger), into your products and services. You can deliver the assets in real time (called *streaming*) from a IBM Content Manager VideoCharger Server to clients over the Internet, an intranet, or local area network. Streaming from the server eliminates the need to download the assets first and can spare much of the client’s disk space.

Choosing a configuration

There are many ways to configure the Content Manager system:

- You can install all components on a single machine (as you might do for your first prototype Content Manager system)
- You can have each component on its own machine, on different operating systems
- You could have 15 Client for Windows on a number of Windows machines

- You could have five other eClients on various platforms all connected to the same system
- You could have the library server on a Windows machine and have your resource manager installed on an AIX machine
- You can have your system administration client installed on any one of your existing machines, or on its own.

In summary, your configuration could be described as one of the following:

- An entire Content Manager system on a single Windows workstation.
- A large system with components on separate machines and with some components on different operating systems.
- A medium-sized system with some components combined, and some components on their own systems. Some components are on different operating systems.

Figure 5 on page 12 shows how all possible components connect together to make up a full Content Manager system.

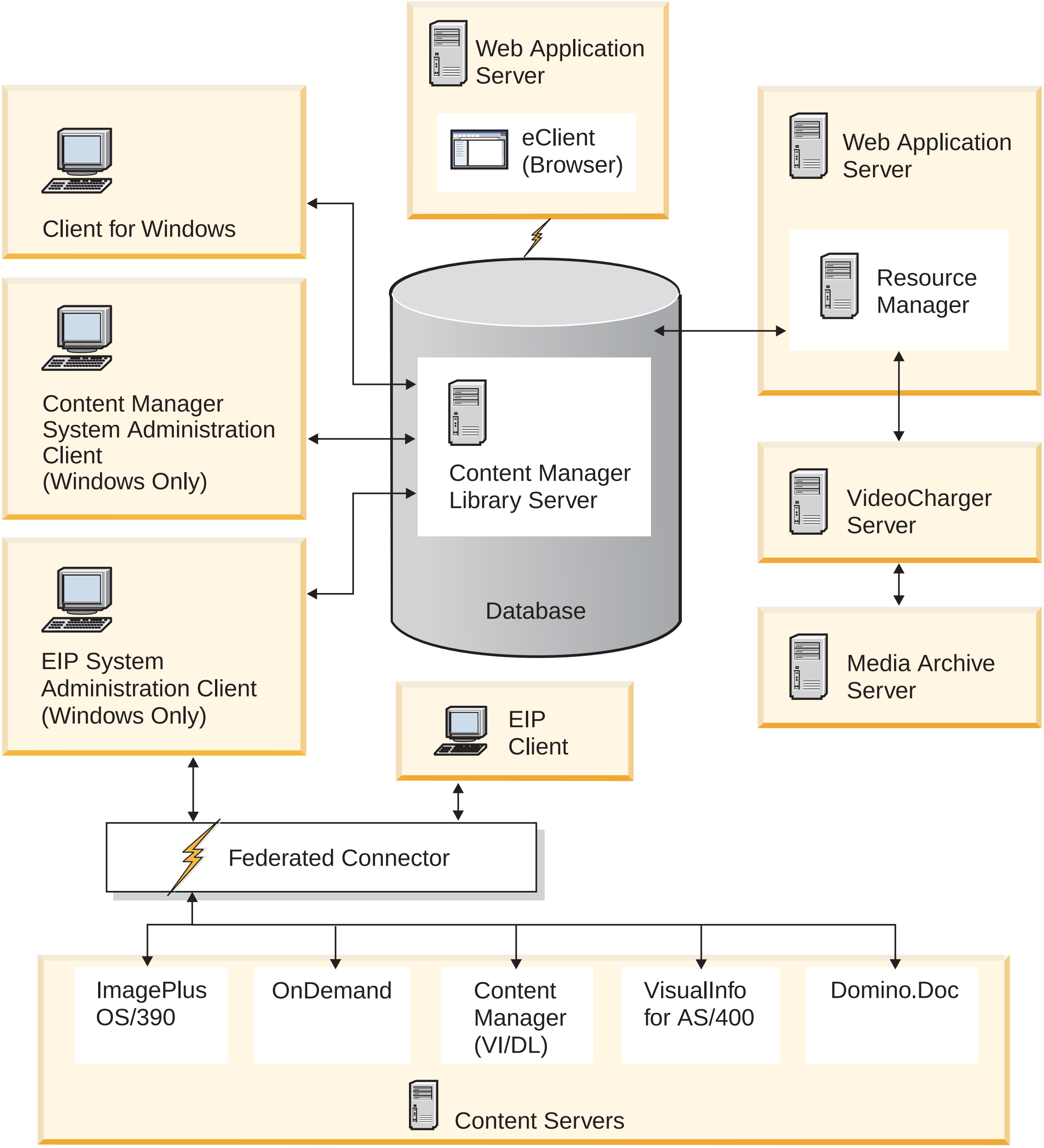

Figure 5. Full Content Manager configuration

Content Manager and e-business

E-business requires more than a web site. At its heart, e-business demands integrated access to information across departmental boundaries, and even between companies. This information is not limited to the structured data kept in various databases and backend systems, but includes the wide array of customer communications:

- applications
- order forms
- statements
- invoices
- shipping documents
- correspondence and e-mails that enable the transaction and support the customer relationship.

In the shift from paper-based commerce to e-business, these documents have not gone away. In e-business, electronic and document-driven processes instead intertwine, so the new challenge for companies is how to integrate paper's digital equivalents, or e-documents, into their e-business strategies.

IBM Content Manager Version 8 Release 2 meets the challenge by providing the technology you need to store and manage information, both data and documents, in a way that supports the integrated access needs of e-business. Content Manager technology provides secure, scalable, storage and management of vast amounts of information, both structured and unstructured, across a wide variety of data types and formats. The Content Manager solution makes information easily searchable and accessible across the Internet, and integrates the information with your specific e-business processes.

IBM Content Manager for Multiplatforms is making it easier for companies to incorporate documents and historical data in a wide array of front office and web self-service applications. Content Manager covers a vast range of content types, from paper and fax to E-mail to statements and invoices to multimedia, providing repositories tailored to the unique characteristics of each type but all accessible through a common API and unified search and retrieval.

Content Manager and the insurance industry

For industries such as insurance, Content Manager offers these benefits:

- Provides real-time, online access to policy, claims and customer information
- Consolidates integrated information in diverse formats into a common repository for enterprise-wide management and retrieval

- Automates underwriting, benefits administration and other time-critical business processes
- Offers Web-based customer service and support

Insurance companies are not only experts in providing their customers with peace of mind, but they must also be savvy at managing valuable information from a myriad of sources. All of the activity that goes into protecting people's interests involves documentation, and plenty of it. Information is collected every time a policy is quoted, a statement is sent, or a claim is paid.

Business information is no longer restricted to documents. Digital video, high-resolution photographs, and spreadsheets can also be vital resources for the insurance industry. To provide the kind of service that helps you attract (and keep customers), you need to integrate these diverse information sources, and provide underwriters, agents, and brokers a comprehensive overview of customer cases quickly and conveniently.

By removing the limitations of routing paper and aggregating relevant content into a dynamic virtual client folder, Content Manager can bring value to a variety of insurance applications, including:

- Individual life underwriting
- Group pension plans
- New policy applications
- Customer service
- Diversified claims processing and inquiries
- Complex underwriting and litigation support

Customer-facing representatives and claims adjusters in the insurance industry can use the Content Manager solution from their desktops, anywhere in the world. They can use it to retrieve anything (within seconds) that they need to perform their jobs, such as:

- Video testimonials about accidents
- Images of damaged vehicles
- Statements
- Invoices
- Correspondence related to accidents

Content Manager and the customer service industry

Nowhere are the benefits of Content Manager more applicable than in customer service. When your customer service representative (CSR) takes a phone call from an end-user, neither cares about the source or medium of the required information. The caller needs help and the service representative wants to deliver it.

Content Manager delivers many features to help build solid, positive customer service operations, including:

- Document management capabilities, with version control, check-in/check-out and Open Document Management API (ODMA) support integrated into a single server
- Support for diverse content types (including images, facsimiles, spreadsheets, desktop documents, streaming audio/video with a transparent player)
- e-business enablement with the Content Manager eClient
- Replication for resource manager for enhanced availability

Users in the customer-service industry can use Content Manager to build customer satisfaction through easy, dynamic access to all customer-related e-content and increase productivity of customer service representatives.

Content Manager integrates scalable, reliable, secure e-content management into core business processes and customer relationship management (CRM) solutions.

Too often, customers bear the burden of helping customer service representatives (CSRs) piece together information about themselves. The company probably already has the information but just can’t seem to find and gather it together. From statements, invoices, insurance policies, checks or any number of applications that use paper-based correspondence and e-mail, business content in the commercial world exists in many unstructured formats. In fact, more than 85 percent of today’s business information resides in sources outside of traditional databases.

Content Manager allows CSRs to quickly access digital versions of customer interactions when responding to requests for documents, improving productivity, response time and overall customer service.

Chapter 2. Introducing the XYZ Insurance scenario

The following scenario about a fictitious insurance company illustrates a basic implementation of Content Manager, VideoCharger™, and Enterprise Information Portal. Use this scenario to assist you with planning, administering, and implementing your Content Management solution.

Background

XYZ Insurance (XYZ), a large auto insurance company, has an extensive collection of photographs, claims, policies, adjuster's notes, reports from experts, and other documents. It is a large organization with offices in various locations around the country and many employees who need quick access to documents stored in various media--Internet, network, and so forth.

The business need

XYZ Insurance kept a majority of its information in physical filing cabinets, which involved the time-consuming task of filing documents, and had some digitized information in a wide variety of media types. Its paper files had become unmanageable and any video documentation became lost in storage. This system made finding misfiled documents difficult and led to poor productivity. XYZ Insurance wanted a system to manage customer information and gather it quickly from different systems throughout the company. It needed a single Web interface to access client information for all its employees. XYZ Insurance wanted to have a low cost information management system, reduce operation costs, improve customer service, and increase market share.

The solution

XYZ Insurance deploys IBM Content Manager for Windows NT®, VideoCharger, EIP, and eClient. It uses these products because it has components that work together to provide solutions that are uniquely suited to its business needs. They use Content Manager to scan insurance applications, enter customer information into databases, and conduct workflow. Any video documentation they receive, they store on VideoCharger. EIP is used as the middleware to access all the backend Content Manager databases. The eClient allows remote offices to access information via the Web.

With this solution in place, employees can search for information, enter any new information, and respond to customers in a timely manner. Document retrieval is now both simple and accurate and employees can maintain all information with 100% integrity. XYZ Insurance can manage more documentation as a result, because it no longer needs to have employees file paper documents or retrieve misplaced documents, thus, increasing its market share.

Setting up the system

This section explains the steps that XYZ Insurance had to take to implement its new system. For example, the databases they use, the environments they need to work in, and so forth.

Planning and designing the data model

Before you define your Content Manager system, you need to plan your entire system. Planning your system includes analyzing your business process, deciding which users require access to the objects on your system and what type of access they require, how objects are migrated from one storage medium to another, and how objects are defined for search and retrieval.

Even if you are sure that you understand the current business needs in your department or group, have your users keep a daily log of their tasks. You might uncover something new about how your coworkers really perform their work.

Administering your Content Manager system

When you have analyzed and planned out your Content Manager system, the system administrator must define the Content Manager elements in the following order:

1. System-managed storage
2. Privilege sets
3. User IDs
4. Access lists
5. Administrative domains
6. Item types
7. Work Nodes
8. Document routing

As a system administrator, you define system-managed storage, which includes setting up and managing the library server and resource managers, you set up and manage object storage and retrieval, user access, and document routing. Depending on the scope of your tasks, you might have to work with a DB2 administrator to keep up the integrity of the objects that users store on the DB2 database. You might also work with other content server administrators, for example, the EIP system administrator, to maintain content server mappings.

For more information about how to set up a Content Manager system, refer to the *System Administration Guide*.

Customizing your system

XYZ Insurance has a complex desktop application that meets some very specific business requirements. XYZ Insurance employees have used the custom application extensively and have become accustomed to using its extensive set of features and capabilities. Therefore, XYZ Insurance chooses to integrate their application into their newly established Content Manager system instead of creating a completely new application. This is easily done using the comprehensive, easy to use set of development tools provided by Content Manager.

An XYZ Insurance application programmer evaluates XYZ Insurance's application and determines that in order for XYZ Insurance employees to perform their daily tasks, they need access to a customer's policy data, like the policy terms, photos, letters, and so forth. The programmer also determines that XYZ Insurance stores all of its customer information in folders of item type policy. Therefore, using the policy number provided by the end user, the application has to retrieve the corresponding policy folder from the Content Manager system. The folder and the list of all its contents must be retrieved from the Content Manager system quickly so that the information can be presented by the application to the end user for viewing, processing, and storing.

XYZ Insurance's application programmer analyzes the Content Manager development tools and quickly adds the additional capability into their application. For more information about the Content Manager development tools, see the Working with Content Manager Version 8 Release 2 section of the *Workstation Application Programming Guide*.

Integrating IBM Content Manager VideoCharger into your system

XYZ Insurance's system administrator installs VideoCharger on another server in order to store and stream media files (audio and video). Using a VideoCharger Player client application, numerous Windows workstations can watch videos in real-time without having to download them first. For details, see *Planning and Installing VideoCharger* and the *VideoCharger Administrator's Guide and Reference.*

XYZ Insurance decides to utilize Content Manager's administrative capabilities to manage videos the same way it would manage documents and photographs. The administrator logs into the library server system administration window and adds the VideoCharger Server to an already existing resource manager. Content Manager then treats the VideoCharger Server as another resource manager. For details, see *Planning and Installing VideoCharger*.

XYZ Insurance's application programmer writes an application that lets an end user pick a media file in Content Manager that would automatically stream using VideoCharger. The programmer uses a Play API to send a temporary metadata file to the client workstation which would initiate streaming. The programmer also uses a Retrieve API to allow the option of exporting the media file to an FTP site. For details, see the *VideoCharger Programmer's Reference.*

Administering your Enterprise Information Portal system

XYZ Insurance deploys Enterprise Information Portal because the comprehensive search technologies allow them to connect and search all of their content servers for the retrieval of data. Now, when an XYZ Insurance Call Center representative receives a call, a single federated search retrieves all of the necessary policy holder information.

Using the eClient

In order for XYZ Insurance employees to provide customer service, they have a need to simultaneously access all customer information. This information is located in a variety of different content servers including IBM Content Manager. An EIP administrator can set up and administer the searches XYZ Insurance employees perform across different content servers. The employees can access the customer information in these servers through a Web browser, using the eClient. Because the eClient is conveniently accessed in a Web browser, the company does not have to install a client at every machine in all of the XYZ Insurance insurance branch offices. Through the eClient, employees can search, create, delete, and display documents and folders stored in these servers, and start and process workflow.

An XYZ Insurance web administrator installs the eClient using the *Installing, Configuring, and Managing the eClient* document and configures it as a Web application. The administrator defines workflow process, enables e-mailing of retrieved documents, and might also customize the eClient. When employees use the eClient, the search templates available to them are retrieved from the EIP system administration database. They select a search template and enter values for the search criteria and run the search. A list of documents satisfying the search criteria are returned to them. Once employees have located documents, they can print or e-mail them or start them on a workflow. They can view a broad range of document formats such as MOD:CA, TIFF, JPEG, and GIF using either a server side conversion or an applet viewer.

If XYZ Insurance decides it does not want to use EIP to build search templates, the eClient can also directly connect to a single content server using a connector. For example, if the EIP administrator installs a Content Manager connector, employees can perform searches on information stored in Content Manager by selecting an item type to search on. EIP search templates and user IDs (that map to the Content Manager server) do not need to be defined.

Chapter 3. Planning for Content Manager

This section is provided to help you plan for the key components of Content Manager. Your IBM sales representative can work with you during the planning process to provide more detailed information about planning considerations. Requirements for Content Manager components are shown in Chapter 6, “Content Manager hardware and software requirements”, on page 55.

General planning for system configuration and user management

During the installation of Content Manager, you will be asked to supply information or make various decisions about options. In many cases, you can take the default name, path, or option, or you can change them if you need to. Whether you take the default or make a change, it is often very important to remember the decisions that you make (for use at a later time), like the following:

- The location of your configuration files
- The names of your various databases
- Certain keywords

To help you remember key data, we have provided special charts within the ″Install″ sections of this guide for you to record this important information.

It might be useful for you to review these sections in advance and print copies of them. Then, you can use them during the install process to keep track of your decisions.

Planning for LDAP (Lightweight Directory Access Protocol)

During the Content Manager installation, you decide if you are going to use the standard method for managing users or if you are going to use LDAP (Lightweight Directory Access Protocol). You can decide to enable LDAP at that time, or you can decide to enable it later by using the LDAP Enable utility described in “Enabling LDAP” on page 482.

If you want to take advantage of LDAP with Content Manager, there are three possible ways that it can be implemented:

- Use the IBM Directory Server. See “Planning for IBM Directory Server” on page 24.
- Use the Active Directory of Windows 2000. See “Planning for Active Directory (Windows 2000 only)” on page 24.

- Use Lotus Domino Directory Notes™ Address Book (NAB)

Planning for IBM Directory Server

IBM Directory (known as IBM SecureWay® Directory in previous versions) is a Lightweight Directory Access Protocol (LDAP) cross-platform, highly scalable, robust directory server for security and e-business solutions.

The IBM Directory product is available in this package with Content Manager. Use the documentation provided on the product CD to plan and install IBM Directory. It can be installed at any time, that is, you can implement and enable it at any time, either before or after you install Content Manager.

Planning for Active Directory (Windows 2000 only)

Active Directory is the name of the LDAP directory used by Microsoft for Windows 2000.

If you are running Windows 2000 Server, you can use the Active Directory feature as your LDAP method with Content Manager.

If you plan to use the Active Directory feature, you must adhere to the following rules:

- There must be an Active Directory set up according to the procedures in the Microsoft Windows 2000 server documentation.
- The system used for Content Manager must be able to physically access an Active Directory server. To verify this, open the command prompt window and enter: `ping <ip address>`

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 address book. See the Domino Directory documentation for more information about implementing LDAP with Domino Directory Notes Address Book.

Planning for performance and scalability of Content Manager

The process for ensuring that a production Content Manager system will have acceptable performance and scalability includes more than modifying tuning parameters after installation. Information is provided in this section to help you start planning for performance and includes:

- A description of recommended best practices in “Performance methodology” on page 25.
- Hints for “Planning for a library server” on page 26.
- Hints for “Planning for resource managers” on page 26
- “Configuration choices and tradeoffs” on page 27.

- A section that tells "Where you can find more information about performance and tuning" on page 29

Performance methodology

This section provides an overview of recommended performance "best practices" with the primary goal of avoiding surprises later on. Its scope ranges from the very beginning of planning for a Content Manager system through to the routine monitoring of the production system. It also includes an overview of the configuration and application design choices a CM administrator faces, focusing on the performance implications of those choices. Recommendations:

1. Read and understand the (XREF to configuration choices and trade-off in this document).
2. Plan and document your overall system topology and configuration.
3. Understand and document your projected workload, and you performance and scalability objectives:
   - Number of desktop and web client users
   - Frequently performed operations (for example: search, view, import, doc-routing) by ″typical users″.
   - The number of operations performed per hour during ″peak hours″
   - Average document size and number of pages
   - Use of features with significant performance impact (for example, mid-tier conversion, migrator, versioning, custom clients, or custom data models)
4. Your IBM representative has a "sizer" tool to help you make an initial rough sizing of the hardware configurations that should be able to support your workload.
5. Read and understand the performance tuning recommendations in this document. Be aware that performance tuning involves trade-off -- appropriate tuning techniques and parameter values depend on the unique circumstances of your configuration and workload.
6. Plan for an initial tuning period to maximize confidence and reduce risk before going into production. If possible, use automated test tools to drive a multiuser test load based on your projected workload. During this tuning period iterate focusing on one area at a time, changing only a small number of tuning parameters. Run the test workload to evaluate the effect of each set of changes before making additional tuning changes.
7. In production, perform routine performance "maintenance", and monitor the performance of your Content Manager server systems:
   - Perform periodic database "runstats/rebind", as described in the tuning recommendations.
   - Maintain a periodic performance profile of key performance metrics (CPU, memory, network, and disk utilizations, for example, as well as

overall throughput and the response times for key operations), using the available performance monitoring tools on your platform.

- Validate your original workload projections against your production system.
- Document the performance profiles over time to observe trends before they become a problem.

Planning for a library server

The library server is the component of a Content Manager system that stores, manages, and provides access control for items stored on one or more resource managers. The library server processes requests (like update or delete) from one or more clients and maintains data integrity between all of the components in the Content Manager system. User access to items stored on any resource manager in the system is directly controlled by the library server.

A library server relies on a relational database management system (RDBMS), like DB2 Universal Database, to manage the library contents and perform parametric, text, and combined parametric and text searches. You can access a library server using the client provided by Content Manager, direct SQL (Structured Query Language), or a relational database client. A Content Manager system requires one library server, which can run on the Windows, AIX, or Solaris operating system.

Planning for library server capacity

Library servers build search requests and transmit search results to the client. You must allocate storage for the database as it grows. Make sure you reserve disk space for prerequisite software and the Content Manager program files.

Library server machines have a high reading and writing work load, and they require a powerful processor to accommodate concurrent requests from multiple users. Because the database is at the core of the library server, good database administration is crucial to the library server's efficient operation.

Planning for resource managers

The resource manager is the repository for objects stored in the system. Users store and retrieve digital objects in the resource manager by routing requests through the library server.

The resource manager efficiently and automatically manages storage resources, based on the storage management entities defined using the Content Manager system administration client.

The system administrator can specify how long objects reside in one medium before migrating them to another. After the system administrator defines migration policies, the resource manager automatically manages storage.

For example, a photograph is scanned into the Content Manager system. If the object has been assigned a migration policy, the system checks the migration policy and moves the digital object to the first migration storage location. The system continues to move the object according to the defined storage management policy.

Resource managers can be distributed across networks to provide convenient user access.

Planning for resource manager capacity

To plan the capacity requirements for storing documents in a LAN-based resource manager, you multiply the number of objects by their average size. You then add that result to the hard drive space that is required for:

- Prerequisites and program files
- Staging area
- Growth in the resource manager database

Configuration choices and tradeoffs

This section describes some of the important configuration and application design choices when planning a Content Manager Version 8 system, focusing on the performance implications of those choices.

Web clients or desktop clients?

- Desktop clients are typically faster than web clients
- Web clients are typically easier to deploy and maintain

For web clients: Direct retrieve or mid-tier conversion?

- Direct retrieve is faster and more scalable
- Direct retrieve may require browser plug-ins or viewer applet

For web clients: Direct Connect or Federated access?

- Federated access is slower than direct connection to Library Server
- Federated access supports search across heterogeneous backend servers

IBM client program or custom client program?

- A custom client program can be tuned to your exact requirements
- The IBM clients already use our latest general-purpose tuning methods

For custom clients: Beans (non-visual, or non-visual + visual), or Java/C++ OOAPI?

- Beans implement only the document model
- Beans support rapid application development with a federated “reach”

- OOAPIs will have the best performance

For Java or C++ OOAPI custom clients: Document model or custom data model?

- The document data model already includes our latest general-purpose tuning methods
- A custom data model can be tuned to your exact requirements

Document routing or advanced workflow (MQSeries workflow)?

- Document routing has better performance and higher scalability
- MQSeries workflow offers advanced workflow function not available with doc routing

Versioning

- Versioning increases the library server database size
- Accessing current version is faster than accessing previous versions

Attribute indexes

- Appropriate indexes improve performance of searches and reduce library server resource usage
- Indexes increase library server database size, and affect store and update times

Resource manager asynchronous and third-party ingest/delivery

- Asynchronous and third-party require custom clients
- Appropriate for very large objects, such as for VideoCharger

Library server and resource manager on the same or separate machines

- Higher scalability when on separate machines

Single or multiple resource managers

- Multiple resource managers give higher total bandwidth for larger objects
- Multiple resource managers give higher migrator parallelism
- Distributed resource managers located close to end users provide better performance

Number of resource manager collections

- Multiple collections give higher migrator parallelism (one thread per collection)

Server platform choice

- Mid-tier server
  - CM v8 Java OOAPI supported on AIX, Sun, and Windows
  - Some other connectors are Windows-only
  - Java conversion engine is cross-platform

- library server and resource manager
  - Higher scalability on AIX or Sun than Windows

Where you can find more information about performance and tuning

For more information about performance and tuning, see the Performance Tuning Guidelines that are posted on the IBM Support page for Content Manager under the ″White pages″ category at:

www.ibm.com/software/data/cm/cmgr/mp/support.html

Planning for client and server time synchronization

It is recommended that clients and servers be kept synchronized to UTC time or some other time standard. (There are a number of tools that are available for free to accomplish synchronization.)

Most important: The time difference between the library server and the resource manager should be kept to a minimum to ensure the best operation. While the servers do tolerate normal time variances, there are complex scenerios where the servers may refuse a client operation due to a large differences in time.

Planning for system administration

Use the system administration client to manage your Content Manager system and database utilities:

- To configure the library servers
- To set up and work with the resource managers
- To define user access and control
- To control access to documents
- To set up your Content Manager data model (see “Planning your Content Manager data model” on page 31.)
- To set up document routing

Use the additional planning instructions indicated for any of the following features:

- LDAP - See “Planning for user management” on page 34.
- Text Search - See “Planning for the text search feature” on page 35.

Understanding the basics

The building blocks of content management are items and objects. The easiest way to understand these concepts is to use a metaphor we’re all familiar with: a library. A library is full of information in different forms: books, videos, music, pamphlets, magazines and journals. Generically, each of these pieces of information is an *object*.

To find objects in a library, you look in a catalog. You search for an object by identifying at least one thing that you know about that object, for example, the author of the book. When you search for that author by name, the library catalog provides results. Generically, each of these results is an *item*.

The item is not the object, but thoroughly identifies it and how to find it. Usually, an item directly corresponds to one or more objects (for example, one item might identify one book, or it might identify a set of two videos that make up a complete movie). In some cases, however, an item contains information that does not directly equate with an object. For example, if you look up a broad subject keyword in the catalog, the resulting item might actually be a list of items that further narrow the subject.

Understanding the basics of describing data

To understand the basics of describing data, we start by describing items and item types.

Items hold consistently formatted data that describe and identify data objects. The items are used to help locate objects and to identify objects quickly. The *item type* defines the specific set of information that is required to identify and locate objects of that type (that is: the collection of descriptive tags that are used to identify a group of objects). Using Content Manager, you build item types for recording a consistent set of information about the objects that you want to catalog. Different groups of objects may require different sets of information to be associated with them, and so, they can belong to different item types.

The information recorded in the catalog about each object differs by the type of object. Each item type has an associated *item type classification*, which identifies in a general way, the format of the object. Content Manager supplies the following item type classifications: document, image, video, audio, folder, object, and text; you can also create your own item type classes.

So, for a video, you might want to know the title, duration, and format, whereas for a journal article, you might want to know the name of the journal, number and date of the issue, and the name of the author or authors. Each of these characteristics of the object is an *attribute*.

When you build an item type, you specify the attributes for which your users must enter values to identify objects. Those same attribute values can be used to locate and view the object later. Some attributes logically go together, for example, you might create an item type that includes an address. The address is an attribute grouping, a convenient way to refer to the group of attributes including street, city, state or province, country, and postal code.

Because objects are digitally stored in Content Manager on one or more resource managers, and not physically on library shelves, your item types must also include attributes specific to the format of the objects, for example, an image might be GIF or JPEG. (The format does not affect the item type of an object. An item type may hold objects of any format.)

Planning your Content Manager data model

Based on the organization of the library catalog, you can assume that it did not come into existence by accident. You can assume that some person or persons did some planning before designing the layout of the cards, so they could store their items efficiently in their library and be able to retrieve them quickly.

We could say that the layout on the index cards represent a **data model**, and we could convert the physical card catalog, and the physical library itself into a digital Content Manager library.

Now that you understand the basic concepts of what a data model is, you can begin to define your own model. Look at all of the procedures that your company performs, and at the information that you might store into the Content Manager system. Realize that Content Manager is a very flexible system and it is easy to modify your data model whenever you need to do so. The idea is to get started and to define as much as you can for your basic model.

You can refer to this simple scenario of our fictitious XYZ Insurance Company and some of the things that they might consider when they create their data model.

A more complete scenario is shown in Chapter 2, “Introducing the XYZ Insurance scenario”, on page 17.

Here are some definitions of the key terms that you will use for your data model, and that are used by the system administration client when you define your model to the Content Manager system.

Item Type

A template for defining and later locating like items, consisting of a root component, zero or more child components, and a classification.

For example, you might have an item type called Insurance claim. The Insurance claim item type includes a consistent set of characteristics, or attributes, for example: Policy holder name, Policy holder ID number, Incident date, Vehicle ID number, and so forth. When you create an item of type Insurance claim, you enter values for each of these attributes, and those values that uniquely define that item.

Attribute
An attribute is a unit of data that describes a certain characteristic or property (for example, name, address, age, and so forth) of an item, and which can be used to locate that item. System administrators define attributes, and can specify the type of attribute from a list of available types such as Character, Integer, or Decimal. The system administration program stores these defined attributes and makes them available for selection when creating or modifying item types.

Attribute group
When creating attributes, you usually make them as basic as possible so that they are flexible enough to use throughout your system. You might find that you use a couple of the same attributes for multiple item types. For these attributes, you can create an attribute group. An attribute group is a set of attributes that are grouped together for convenience.

Adding an attribute group to an item type will insert all attributes in the attribute group into the item type at one time. For example, instead of searching for and selecting four attributes for every item type to create an address (street, city, state, and zip code), you create an attribute group called Address that includes those four attributes. When you create an item type, you select the attribute group Address and the system will insert street, city, state, and zip code.

Link A link is used to relate one item type to another item type. For example, if you have an item type called customer, it could link to another item type called address.

Reference
Used with attributes. As the system administrator, you define the delete rules for the reference (if it can be deleted, or if it should never be deleted).

Item An item is a generic term for an instance of an item type. For example, you might have item types called Insurance claim and Policy holder. Each claim that you create and each policy holder that you identify is generically referred to as an item.

The steps that the XYZ Insurance Company might go through to plan their data model might be:

1. They begin by analyzing their business procedures. They look at all types of information that they collect and could store into their Content Manager system. Some of the item types that they have identified are:
   - Application forms
   - Claim forms
   - Accident reports

2. For each item type that they identify, they list all of the possible attributes that could describe the item type. For example, attributes that they identify for the Insurance application form are:
   - Customer name and address
   - The thing that is to be insured
   - The date of the application

   An example for writing the notation for an item type and it attributes might be:

   ```
   application form (name, address, insured item, date)
   ```

   The notation for the claim form could be:

   ```
   claim form (date, policy no., photos, witnesses)
   ```
3. After they list all of the possible attributes, they realize that the customer name and address, and other specific information about their customers will probably be used by almost every other item type that they create. They decide that *Customer information* should be an item type on its own, and that other item types could either reference it or link to it when that information is needed.
4. They look at the attributes that they listed and decide whether some of them can be put together into an *attribute group*. For example, address becomes an attribute group name made up of the four obvious attributes of street, city, state, and zip code.
5. They draw diagrams to show relationships of their items to each other:

   ```
   application form (name, insured item, date)
                              \
                               \
                            customer (name, address)
                             /
                            /
             claim form (policy #, date, pictures)
   ```

Where do you go from here?

After you have defined your processes and identified your item types and attributes and you are ready to create your own data model, go to the ″Getting Started″ section of the System Administration Guide to learn how to enter your data model into the Content Manager system.

Planning for clients

Refer to “Client options” on page 8 for a summary of your options.

When planning for client components, examine what tasks your client will perform. Generally, clients fall into one of three categories:

- Scanning clients, which capture documents into the system

- Display clients, which view or work with objects
- Indexing clients, which create metadata about objects in the system

If your Windows client workstation is not dedicated to Content Manager, ensure that the workstation has enough RAM to prevent the client from being swapped out.

Important: Ensure that the client application that you use is enabled to recognize the item types that you want to use. For example, the clients that come with Content Manager use only the document classification. See the *System Administration Guide* for more information about item type classifications.

Planning to create customized applications with the Enterprise Information Portal ICM Connector

The ICM Connector (when installed with Enterprise Information Portal) enables you to create customized Content Manager applications by using client APIs. You can use APIs to:

- Access information in the library server and resource manager
- Customize document processing
- Design your own data model

Planning for user management

As mentioned earlier in “Planning for LDAP (Lightweight Directory Access Protocol)” on page 23 you decide (during installation) if you are going to use the standard method for managing users, or if you are going to use LDAP (Lightweight Directory Access Protocol). LDAP is described on page 23; the standard method is described here.

When you plan for your Content Manager system configuration and setup, you must also decide who can have access to your system and how much access these users must have to the objects on your system. The Content Manager system defines user access through privileges. A privilege grants the right to access a specific object in a specific way. Privileges include rights such as creating, deleting, and selecting objects stored in a system.

A group of privileges assigned to a user is a privilege set. A privilege set identifies the functions that a user can perform, such as creating folders or adding objects to a work process. A user cannot access the Content Manager system without a user ID, a password, or a privilege set.

Before creating users and assigning them privileges, you must decide who can have access to the system and what their jobs dictate. You do not want users having the right to delete an object when they do not understand the scope of what deleting that object can do. On the other hand, you do not want to prevent users from doing their jobs by not giving them the correct privilege set. So, before assigning users privilege sets, you will need to define the types of tasks each job requires.

Often, users with the same job description have the same or similar tasks, and therefore, they might need the same access to objects on your system. You can group users with common access needs into a user group, but you cannot nest user groups. A user group is solely a convenience grouping of individual users with similar tasks. You do not assign a user group a privilege set. Each user in a user group has his or her own privilege set. A user group makes it easier to create access control lists for objects in your system. When users create an object in the Content Manager system, they must define who can access the object and what operations can be done to the object. This definition is what is known to the Content Manager system as an access control list (ACL).

An access control list is a list consisting of one or more individual user IDs or user groups and their associated privileges. You use ACLs to control user access to objects in the Content Manager system. The objects that can be identified in ACLs are:

- Objects stored by users
- Item types
- Workbaskets
- Workflows
- Worklists

Although privilege sets define an individual user’s maximum ability to use the system, an ACL restricts an individual user’s access to an object. An ACL that has a privilege that is not defined by a user’s privilege set does not grant the user that privilege. Only users that have that privilege can use that privilege on an object. An ACL limits user access, it does not grant more access.

Planning for the text search feature

The optional text search feature allows for full text searching through documents in the Content Manager database.

It allows you to automatically index, search, and retrieve documents stored in Content Manager. It lets you locate documents by searching for words or phrases using a client.

To use it, you must plan ahead and install the DB2 Text Information Extender (TIE) or DB2 Net Search Extender (NSE) when you are installing the prerequisite DB2 software for the library server.

Planning for IBM License Use Management (LUM)

IBM License Use Management (LUM) is the IBM product for technical software license management. The LUM tools are available to help you to comply with the terms and conditions of license agreements. They check compliance through runtime monitoring of the usage of software assets.

You can decide to install LUM at any time, either before or after you install your Content Manager system.

See “Installing and configuring IBM License Use Management (LUM)” on page 500.

Chapter 4. Introducing Enterprise Information Portal

Many paper-intensive enterprises, such as insurance companies and financial institutions, administer large volumes of business-related content. The need for an enterprise solution for managing and accessing business information spans many industries.

A *content server* stores multimedia objects, business forms, documents, and related data. The content server also stores metadata that allows employees to process and work with the content. When there is no way to effectively connect all the information on different content servers, a business can waste time and money by duplicating information or training employees to perform multiple searches.

Enterprise Information Portal provides leading-edge technology to bring all of your enterprise resources to your workstation desktop. EIP can help you maximize the value of your information and multimedia assets by connecting disparate content servers through a single client. With an EIP client, users can quickly and concurrently access information on all connected content servers. Users can also mine information, conduct intelligent searches across content servers (including the Web or an intranet) and perform workflow tasks within your business processes.

With Enterprise Information Portal, you can customize applications for your enterprise by installing the connector toolkit and samples. Application programmers can use the connector toolkit and samples to create desktop and Web-based applications.

Introducing the Enterprise Information Portal components

This section explains each EIP component and describes the installation options.

See Chapter 6, “Content Manager hardware and software requirements”, on page 55 for information on component prerequisites.

Table 3 lists the components and the compatible operating systems.

Table 3. EIP component operating system compatibility

Component	Windows	AIX	Solaris	Notes
Administration database	yes	yes	yes	Database includes workflow builder functionality
Administration client	yes	no	no	Client can connect to databases installed on Windows, AIX or Solaris operating systems.
Connectors	yes	yes	yes	
Information mining server	yes	yes	yes	
Information mining client	yes	no	no	
IBM Web Crawler	yes	yes	yes	
Text search client	yes	yes	yes	
Image search client	yes	yes	yes	
Connector toolkit and samples	yes	yes	yes	• Windows version includes source code to compile sample client. No sample client code installed on AIX. • Workflow samples and APIs are installed with the federated connector sample.

Table 3. EIP component operating system compatibility (continued)

Component	Windows	AIX	Solaris	Notes
Viewer	yes	no	no	Installs OnDemand client and viewer.
Information center	yes	yes	yes	

Administration

The administration component provides the administration database and administration client subcomponents. When you install the administration database, you also install the workflow feature.

Administration database

The administration database is a DB2 database that manages information about EIP users and groups, privilege levels, passwords, user IDs, and other information. The database also provides the workflow and, optionally, the information mining functionality. You can install multiple databases. Each database provides the EIP workflow functionality. If you have a Content Manager Version 8 system, you can share the EIP administration database with the Content Manager Version 8 Library Server database. You can share the database because the Library Server database contains all the information required by EIP.

Administration client

The administration client can be installed only on Windows workstations. You can install multiple clients. If you have a Content Manager Version 8 system as the content server, you can administer EIP Administration database (a heterogeneous / federated data mapping layer) and Content Manager Version 8 backend datastore from the same client.

The client provides the interface that allows the administrator to:

- Define each content server for federated searching.
- Identify native entities and attributes on content servers and map them to federated entities.
- Maintain an inventory for all the content servers defined by the EIP system administrator
- Create search templates.
- Identify and manage users and groups.
- Assign privileges to users and groups.
- Define access to search templates and set conditions on the actions users can take with the information retrieved from a search.
- Design and administer business workflow processes.

Connectors

The connectors provide the communications interface between EIP clients, the content servers, and the administration database. The content server connectors, such as Content Manager Version 7.1 connector, provide the functionality that allows EIP to log in to the server, search for information, and return the information to the administration or end-user clients. The federated connector connects the administration client to the administration database.

EIP provides the following connectors:

- Federated connector connects EIP client to the administration database.
- Content Manager connector for Content Manager Version 7.1 servers.
- Content Manager connector for Content Manager Version 8.2 servers.
- Content Manager OnDemand connector for Content Manager OnDemand Version 7.1.
- Content Manager for VisualInfo™ for 400® Version 4.3, and Version 5.1.
- Content Manager ImagePlus for OS/390 connector for ImagePlus/390 Folder Application Facility Version 3.1, Image Plus/390 ODM Version 3.1.
- Lotus Domino.Doc connector for Domino.Doc Version 3.0a, Desktop Enabler Version 3.0a.

Features

EIP has two optional features:

Image Search client
Provides the interface required to access and administer Image Search functionality on a Content Manager Version 7 content server.

Text Search client
Provides the interface required to access and administer Text Search functionality on a Text Search server.

Content viewer

Installing the OnDemand viewer installs the OnDemand client and other files required to view documents retrieved from an OnDemand server.

Connector toolkits and samples

EIP provides a connector toolkit that includes sample programs you can use to experiment with and test various EIP functions, such as:

- connecting to and disconnecting from content servers
- performing SQL and other sample queries on content servers
- determining content server MIME types, and so forth

Windows connector toolkit

To install the connector toolkit and samples on Windows servers, you must select the Development Workstation machine type. Then select the Connector Toolkit and Samples component. You can install the sample programs for all connectors, or select individual samples to match the connectors you installed.

On Windows servers, connector toolkit sample programs are organized in the following way:

```
c:\CMBROOT\SAMPLES\activex\xx
c:\CMBROOT\SAMPLES\cpp\xx
c:\CMBROOT\SAMPLES\java\xx
c:\CMBROOT\SAMPLES\jsp\xx
c:\CMBROOT\SAMPLES\server\xx
```

where *xx* is the directory name containing the sample programs for each applicable connector, for example, `db2, od, dl`, and so forth.

For instructions about how to use sample programs to verify EIP installation and connect to the EIP federated database, see “Verify connections by running low-level connection tests” on page 195.

On AIX servers, the sample programs are organized in the following way:

```
/usr/lpp/cmb/samples/cpp/xx
/usr/lpp/cmb/samples/java/xx
/usr/lpp/cmb/samples/jsp/xx
/usr/lpp/cmb/samples/server/exit
```

where *xx* is the subdirectory name, such as `beans`, `servlets`, and so forth.

On Solaris servers, the development toolkit is named Content Manager EIP Version 8.1 Development Toolkit Base. The package name is `cmbcomub`. Unlike other EIP components on Solaris, the package is installed as a default and is not a selectable option. The development toolkit base is organized on Solaris servers in the following way:

```
/opt/IBMcmb/samples/java/aa
/opt/IBMcmb/samples/jsp/bb
/opt/IBMcmb/samples/server/exit
```

where *aa* is the subdirectory name, such as `icm`, `beans`, `servlets`, or `servlets`.

where *bb* is the subdirectory name, either `servlets`, or `taglib`.

The sample programs include documentation that describes the programs, and provides the server settings (environment settings, memory, and so forth) required to work with the sample code.

Information center

The information center component contains the Enterprise Information Portal information center. The information center is a Web-based, searchable version of the Enterprise Information Portal library.

Chapter 5. Planning your Enterprise Information Portal system

The following sections provide information to help plan your Enterprise Information Portal system. Your IBM sales representative can provide more details and work with you during the planning process.

Analyzing your business information requirements

Analyze your need to access, search for, retrieve and work with business information. This analysis helps you to decide on the appropriate Enterprise Information Portal configuration. The list below represents some common considerations to help plan the right system for your business:

- The network topology strategy for your enterprise
- Types and quantity of clients to deploy
- Information useful for existing applications already contained in your content servers
- Business processes that use this information
- Number of potential users, their location, and potential network traffic
- Number and types of file formats to search for and display
- Hardware capabilities
- Quantity, version level, and location of content servers
- Average number of users who will simultaneously access one or more content servers

For example, you might decide to use multiple Enterprise Information Portal servers to balance workload across your network. You might have some clients on Windows 2000 and others on Windows 98. You also might decide that only certain clients can access the workflow processes of your business or perform information mining.

Planning a configuration

EIP offers multiple ways to configure a system. When you plan a configuration, you must understand how you want to configure your clients and your servers. You can install all components on a single server (Windows only) or distribute the components across AIX, Sun or Windows servers, or all three. Enterprise Information Portal supports RMI server configurations; see “Remote Method Invocation (RMI) server” on page 45.

Enterprise Information Portal’s architecture gives you the flexibility to design many different system configurations. Ask the following questions to help determine where to install the components:

- Local or remote connectors?
- Multiple RMI servers (an RMI server pool) to improve performance?

Choosing a server configuration

When designing the configuration to support your environment, you determine satisfactory response time. Response time depends on:

- The size of the objects you are searching for and viewing
- CPU speed, memory, disk space, network speed
- DB2 Universal Database (UDB) workload

Evaluate and adjust the possible configurations described in this section according to your unique requirements.

You can choose many ways to configure your servers for Enterprise Information Portal, depending on your environment. The following sections describe these possible configurations for your servers:

- Full server
- Administration server and information mining server
- RMI server
- RMI server pool
- Web server
- Workflow server

Full server (Windows only)

The full server configuration consists of one server that includes all prerequisites and all EIP components. The full server is only available on Windows operating systems, because the administration client is only compatible with Windows operating systems. A full server would include:

- IBM DB2 UDB
- WebSphere Application Server
- MQSeries® Server and MQSeries Workflow
- Administration database and client
- Local and remote connectors
- Content viewers
- Connector toolkit and samples
- Information Center
- Information Mining
- IBM Web Crawler

A full server configuration can be used to develop applications, learn the product, or perform a trial run of Enterprise Information Portal. However, consider installing Enterprise Information Portal on a distributed set of workstations to support multiple users with reasonable performance.

Administration server (Windows-only configuration)

You can configure one server to provide administration services by installing only the administration client, database, and federated connector on a single server. The administration server configuration is only compatible with Windows servers because the administration client is a Windows application.

Administration server (multiplatform configuration)

To configure a multiplatform administration server, you install the administration and federated database and connectors on AIX or Solaris, and install the administration client on Windows. An RMI server or DB2 UDB Client Configuration Assistant is required to connect the EIP administration client to the database.

Workflow server

Each administration database contains the tables required by EIP workflow. You can configure one server to support workflow. This is the recommended configuration. Workflow requires IBM MQSeries Server, IBM MQSeries Workflow, DB2 UDB and an administration database.

Remote Method Invocation (RMI) server

You can configure an RMI server to distribute client requests to components. See Chapter 7, "EIP hardware and software requirements", on page 67 for the prerequisites to configure RMI servers on AIX, Windows or Solaris platforms.

This section provides some guidelines for planning an RMI server. With RMI, you can create Java applications that communicate and pass objects to other Java applications over a network.

RMI allows multiple EIP clients to search content servers through connectors installed on one RMI server. If you choose a system that includes an RMI server, you do not have to install the remote connectors on each client. The RMI server supports the connectors, and EIP clients access the connectors on the RMI server when performing a search.

If you plan to use RMI to connect clients to content servers, you do not need the remote content server connectors on EIP client machines. You must write all custom client applications in Java to take advantage of RMI.

RMI server pool

You can configure Enterprise Information Portal with multiple RMI servers to distribute client requests. A group of RMI servers is an *RMI server pool*. When a client communicates with an RMI server, this RMI server can delegate the client request to other members of the server pool. In this scenario, this RMI server acts as a master server. The master server itself fulfills client requests when all the server pool members reach their maximum number of connections.

The clients and the Web server connect with an RMI server in an RMI server pool configuration. Because all remote connectors can be shared on the RMI server, the RMI server pool configuration is scalable and easy to maintain.

Choosing a client configuration

EIP provides an administration client, and also includes code you can compile to create a desktop client. When you install EIP on Windows, the installation program gives you a Client installation option. If you select that option, you can install the connectors and other components that will support an end-user client.

The EIP installation programs on Windows and Sun does not give you the option to install Local or Remote connectors. When you install EIP connectors on AIX, the installation program gives you the choice to install local and/or remote connectors.

You can choose to configure your clients as one or any of the following types:

Client using local connectors

Configure your client with the local connectors if you want your client to connect directly to one or more content servers. A client with local connectors can improve response time, but can require more disk space and a faster processor. This configuration requires you to update all clients when you add or upgrade the content server associated with the appropriate connector.

Client using remote connectors

In this configuration, you install only the client application and remote connectors on a workstation. The client accesses the content servers through an RMI server. This configuration eliminates the need to upgrade remote connectors when systems change, but can worsen response time.

Client using local and remote connectors

Enterprise Information Portal supports client configurations that include both local and remote connectors. Choose this configuration if you want your client to connect directly to some local content servers and connect remotely to others.

Understanding Windows server machine types

When you install EIP on a Windows workstation, the installation program requires you to select a machine type. When you install EIP on AIX and Sun Solaris, you do not select a machine type. This section describes the machine types and has a table showing which components are available with each machine type.

Each machine type provides a specific group of components that support the system configurations described in “Introducing the Enterprise Information Portal components” on page 37. The machine types are EIP Client, EIP Server, and EIP Development Workstation. See Table 4 for more information.

It is essential to understand how the components offered by the three machine types fit into your system design. For example, if you select the Client machine type, you could install the components required to support an end-user client, but you could not install an administration database. If you select EIP Server to install the components that would support a full server or distributed server. If you select the Development Workstation machine type, you can install sample code that can help you program custom applications, such as end-user client. The EIP Client machine type provides the components required for client-only configurations.

Table 4 lists the components offered by the three machine types.

Table 4. Components and machine types

Component	**Machine Type**		
	Client	**Server**	**Development Workstation**
Administration	no	yes	yes
Connectors	yes	yes	yes
Features	yes*	yes	yes
Content Viewers	yes	yes	yes
Connector Toolkit and Samples	no	no	yes
Information	no	yes	yes

* If you select the Client machine type, you can install only the Information Mining, Text Search and Image Search clients. If you select either the Server or Development workstation machine types, you have the option to install both the Information Mining client and he Information Mining server.

Planning system administration

You use the administration client to set up and manage your system. System administration tasks include defining federated search templates, managing information mining and workflow features, and managing access control. You can install multiple administration clients on additional Windows workstations.

The following list includes some high-level tasks to complete when planning for system administration:

- Identify the content servers where information is stored
- Identify the users who can access content server data through Enterprise Information Portal
- Determine what level of security access users and user groups should have
- Define user groups who can access certain search templates
- Identify users who can perform information mining
- Define users and user groups who can perform tasks related to the business and workflow processes of your enterprise

See the Enterprise Information Portal online help for details about how to perform these system administration tasks. See *Managing Information Integrator for Content* for information about concepts behind the administration tasks.

Planning Enterprise Information Portal network security

This section lists six topics to consider when planning Enterprise Information Portal network security.

Authorization

- How do you ensure that users are who they claim to be?
- How do different elements in the system locate and determine whether to trust one another?
- How do you enable new employees, customers or business partners to access existing systems without major changes to existing security infrastructure?
- Whose identity should be used to determine authorization: the end user, the server, or some other entity?

Asset Protection

- Can you keep data confidential and private when it's stored and when it's traveling across relatively untrusted networks?
- How can you be sure that the data doesn't change while it's stored or in transit?

Accountability

- How can you can tell who did what and when?
- How can you ensure, and prove, that requests and results are not altered, inadvertently or maliciously?

Administration

- Can you define the security policy?
- Can you ensure that policies are consistent across all elements of applications, systems, platforms, and networks?

Assurance

- How will the system keeps its security promises?
- How can you ensure that the infrastructure and application resources -- including systems, networks, and data -- are not presently under attack?

Availability

- How do you prevent attacks on elements of the system that cause disruptions in service?
- How do you design for fault tolerance and ensure that applications and data are restored in the event of a serious failure?
- How can you keep the system up and running and also make needed modifications to the application, the systems, and the enterprise network?

Enterprise Information Portal security prevents these three types of security risks:

- Unauthorized network access to Enterprise Information Portal machines, clients, and features
- Unauthorized access to Enterprise Information Portal functionality
- Unauthorized viewing and use of content server information

General planning hints and tips

Enterprise Information Portal supports multiple databases. The databases are independent of each other. Multiple databases provide scalability and increased security. You can install multiple databases on one DB2 system. Enterprise Information Portal provides a utility to create databases after the initial installation.

Check the software version levels of the content servers to which you plan to connect to be sure the levels are compatible with the version level supported by the EIP connectors. For example, if you install the VI/400 connectors, you must select a version number to ensure that you install the compatible connector.

If you install a VisualInfo for AS/400® connector on any platform, the installation program prompts you for information that is stored in the AS/400 network table (frnolint):

- Version number
- Server name
- Host name
- Port number

EIP uses the data in the network table to connect to the AS/400 content server. The network table (`frnolint.tbl`) is installed in `cmbroot`.

Depending on the operating system where you install the OS/390 connector, the installation program might prompt you for connector parameters, such as IP address and other information. But you must know the information listed below to define a connection to the OS/390 server using the EIP administration client:

- FAF port number
- FAF application ID
- FAF protocol
- FAF IP address
- Object distribution manager CICS
- Object distribution manager IP address
- Object distribution manager port number
- Object distribution manager terminal ID
- Additional parameters (optional, depending on OS/390 server settings)

If you install the Content Manager Version 7 connector, you can also install Text Search and Image Search, two optional features.

To install the text search feature, you must know the following information to correctly configure the text search client settings:

- Text search server User ID
- Text search server name
- Text search server hostname
- Text search server port number
- Global setting

To install the image search feature, you must know the following information to correctly configure the image search client settings:

- Configuration file path information (must match the settings defined on the installation panel path definitions for CMBROOT)

- Image server name
- Image server hostname
- Image server port number
- Database name of the Content Manager Version 7 database associated with the image server.

To access DB2 DataJoiner®, make sure the authentication method for Enterprise Information Portal is `server` for the database defined in DB2 Universal Database.

Before you install Enterprise Information Portal Version 8 Release 2, use the Enterprise Information Portal Version 8.1 Uninstall program (or the AIX/Sun equivalent) to remove earlier versions of Enterprise Information Portal components.

Tip: Do not use Windows Add/Remove programs because it does not remove all EIP components.

If you installed the information mining feature with EIP in an earlier release, the information mining database (information mining database) is deleted when you remove EIP. If you want to keep data in this database, back it up before you uninstall. In a db2cmd command window enter `db2 list db directory`. If `IKF` appears in the returned list of databases, the information mining database exists. In the DB2 Command Window, type `db2 backup database IKF to <dir>` where `<dir>` is a directory of your choice.

Planning workflow

In Version 8.2 workflow is not a selectable feature.

Workflow samples and APIs are installed when you select the Connector toolkit and samples component and also select the Federated Connector option.

The workflow builder is installed with the administration client and the workflow functionality is administered through the administration client.

Planning information mining installation

The Information Mining server is always located on the workstation where the administration database is located. If you want to access the Information Mining feature, especially if you want to install the Information Structuring Tool on a different workstation, you must install an information mining client and configure an RMI connection.

Planning EIP performance

This section describes some of the important configuration and application design choices when planning an EIP system, focusing on the performance implications of those choices.

Web clients or desktop clients?

- Desktop clients are typically faster than web clients
- Web clients are typically easier to deploy and maintain

For web clients: Direct retrieve or mid-tier conversion?

- Direct retrieve is faster and more scalable
- Direct retrieve may require browser plug-ins or viewer applet

For web clients: Direct Connect or Federated access?

- Federated access is slower than direct connection to Library Server
- Federated access supports search across heterogeneous backend servers

IBM client program or custom client program?

- A custom client program can be tuned to your exact requirements
- The IBM clients already use our latest general-purpose tuning methods

For custom clients: Beans (non-visual, or non-visual + visual), or Java/C++ OOAPI?

- Beans implement only the document model
- Beans support rapid application development with a federated "reach"
- OOAPIs will have the best performance

For Java or C++ OOAPI custom clients: Document model or custom data model?

- The document data model already includes our latest general-purpose tuning methods
- A custom data model can be tuned to your exact requirements

Document routing or advanced workflow (MQSeries workflow)?

- Document routing has better performance and higher scalability
- MQSeries workflow offers advanced workflow function not available with doc routing

Versioning

- Versioning increases the library server database size
- Accessing current version is faster than accessing previous versions

Attribute indexes

- Appropriate indexes improve performance of searches and reduce library server resource usage
- Indexes increase library server database size, and affect store and update times

Server platform choice

- Mid-tier server
  - CM v8 Java OOAPI supported on AIX, Sun, and Windows
  - Some other connectors are Windows-only
  - Java conversion engine is cross-platform
- library server and resource manager
  - Higher scalability on AIX or Solaris than Windows

Locating more information about performance planning

For more information about performance and tuning, see the Performance Tuning Guidelines that are posted on the IBM Support page for Content Manager under the ″White pages″ category at www.ibm.com/software/data/cm/cmgr/mp/support.html:

Chapter 6. Content Manager hardware and software requirements

This section describes hardware and software that are required to install and run a Content Manager system. Your Content Manager system might require additional hardware, such as optical, tape library, RAID, or other storage devices, for use with resource managers.

> **Important**
>
> See the README for the latest version requirements of prerequisite software, including related update or fixpack levels.

Windows requirements

Before you install any Content Manager components for Windows, ensure that your workstation has the correct hardware and software installed. This section lists the required hardware and software for installing and running the server and client components.

Windows server hardware requirements

Table 5. Required hardware for servers on Windows

Component	Required
Processor	Intel Pentium® 800MHz or equivalent.
RAM	128 MB for each library server 512 MB for each resource manager
Storage	100 MB combined (for the installed product) of: • The library server • The resource manager **Recommended:** • Allow for 300 MB of physical paging space for each server. • Allow for additional hard disk space for data storage.
Display and adapter	SVGA (800 x 600 resolution and 256 color mode)
Other required hardware	• Mouse • CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations)

Windows server software requirements

Table 6. Required software for the servers on Windows

Component	Required
Operating system	Microsoft Windows NT 4.0 with service pack 6 or later, or Windows 2000 Server or Advanced Server or .Net Server 2003 (when available)
Network Communication	TCP/IP installed with Windows
Library server	Microsoft Visual C++ Version 6.0 or Microsoft Visual Studio .Net Professional **For DB2:** IBM DB2 Application Development Client (known as DB2 Software Development Kit, or SDK, in previous versions of DB2)
Library server database	**IBM DB2:** IBM DB2 Universal Database (DB2 UDB), Enterprise Edition Version 7.2 or later or IBM DB2 UDB Enterprise Extended Edition Version 7.2.1 or later **Or Oracle:** Oracle Version 8.1.7.4 or later (for Version 8i) or Oracle Version 9.2.0.1 or later (for Version 9i), and IBM DB2 UDB Version 8.1, and IBM DB2 UDB Relational Connect Version 8.1 **Optional** If you plan to use the text search feature: • IBM DB2 Text Information Extender (TIE), Version 7.2 with IBM DB2 EE or EEE Version 7.2 • or IBM DB2 Net Search Extender (NSE), Version 8.1 with IBM DB2 ESE, Version 8.1.
Resource manager	WebSphere Application Server (WAS) Version 4.0.5 Advanced Edition (AE) or Advanced Single Server Edition (AES) or later **For Oracle** JDBC Driver Version 9.0.1

Table 6. Required software for the servers on Windows (continued)

Component	Required
Resource manager database	**IBM DB2:** IBM DB2 Universal Database (DB2 UDB), Enterprise Edition Version 7.2 or later or IBM DB2 UDB Enterprise Extended Edition Version 7.2.1 or later **Or Oracle:** Oracle Version 8.1.7.4 or later (for Version 8i) or Oracle Version 9.2.0.1 or later (for Version 9i)
Resource manager auxiliary device support	Tivoli Storage Manager API Client Version 4.2.1 (or later) and Tivoli Storage Manager Server Version 4.2.1 (or later) if you want to provide long term storage for your objects on devices other than the fixed disks attached to the resource manager
LDAP	IBM Directory Server 4.1
LUM	IBM License Use Management (LUM) 4.6.2 or later

Client for Windows hardware requirements

Table 7. Required hardware for the Client for Windows

Component	Required
Processor	Intel Pentium or equivalent
RAM	256 MB
Storage	64 MB **Recommended:** Allow for sufficient temporary space for documents being viewed.
Display and adapter	VGA (800x600 resolution and 256 color mode)
Other required hardware	• Mouse (for installation) • CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations) • ASPI-compliant SCSI adapter for scanning

Client for Windows software requirements

Table 8. Required software for the Client for Windows

Component	Required
Operating system	Windows NT Version 4.0, or Windows 2000 Professional, Server, or Advanced Server, or Windows Millenium Edition, or Windows 98, or Windows XP
Network Communication	TCP/IP (included with Windows)
Connector software	**For CM Version 8.1 servers using DB2 Version 7.2, you need:** • DB2 Version 7.2 client software **For CM Version 8.2 servers using DB2 Version 7.2, you need:** • DB2 Version 7.2 client software **For CM Version 8.2 servers using DB2 Version 8.1, you need:** • DB2 Version 7.2 client software • or DB2 Version 8.1 client software **For CM Version 8.2 servers using Oracle, you need:** • DB2 Version 8.1 client software For more information see the "Client/Server support matrix" on page 76.

System administration client hardware requirements

Table 9. Required hardware for the system administration client

Component	Required
Processor	Intel Pentium 800 MHz processor or equivalent
RAM	128 MB
Storage	35 MB for the installed product
Display and adapter	SVGA (1024x768 resolution and 256 color mode)
Other required hardware	• Mouse • CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations)

System administration client software requirements

Table 10. Required software for system administration client

Component	Required
Operating system	Windows NT Version 4.0, or Windows 2000, or Windows XP
Network Communication	TCP/IP installed with Windows
Toolkits	Java Runtime Environment (JRE) 1.3 is installed with this program DB2 Application Development Client • Known as DB2 Software Development Kit, or SDK, in previous versions of DB2 (before Version 7) • Installed automatically as part of DB2 Version 8

Information Center hardware requirements

Table 11. Required hardware for the Information Center

Component	Required
Storage	150 MB

Information Center software requirements

Table 12. Required software for the Information Center

Component	Required
Browser	Internet Explorer, Version 5 or higher Netscape, Version 4.5, 4.6, or 4.7 **Not compatible:** The Information Center is not compatible with Netscape, Version 6.0 or later

AIX requirements

Before you install any Content Manager components for AIX ensure that your workstation has the correct hardware and software installed. This section lists the required hardware and software for installing and running Content Manager components on AIX.

AIX hardware requirements

Table 13. Required hardware for all AIX components

Component	Required
Server	RS/6000® based processor
RAM	256 MB for each library server 512 MB for each resource manager
Storage	100 MB combined (for the installed product) of: • The library server • The resource manager 150 MB for the Information Center **Recommended:** • Allow for 300 MB of physical paging space for each server. • Allow for additional hard disk space for data storage.
Display and adapter	VGA (256 color mode)
Other required hardware	• CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations)

AIX server software requirements

Table 14. Required software for Content Manager servers on AIX

Component	Required
Operating system	AIX 4.3.3 or later versions of AIX
Network communication	TCP/IP (installed with AIX)
Library server compiler	IBM VisualAge® C++ Professional batch compiler, Version 5.0.2.0 or later or VisualAge C++ Professional for AIX Version 6.0

Table 14. Required software for Content Manager servers on AIX (continued)

Component	Required
Library server database	**IBM DB2** IBM DB2 UDB Enterprise Edition Version 7.2 or later or IBM DB2 UDB Extended Enterprise Edition Version 7.2.1 and with the Application Development Client for AIX (known as DB2 Software Development Kit, or SDK, in previous versions of DB2) **Or Oracle** Oracle for UNIX® Version 8.1.7.4 or later (for Version 8i) or Oracle Version 9.2.0.1 or later (for Version 9i), and IBM DB2 UDB Version 8.1, and IBM DB2 UDB Relational Connect Version 8.1 **Optional** If you plan to use the text search feature: • IBM DB2 Text Information Extender (TIE), Version 7.2 with IBM DB2 EE or EEE Version 7.2 • or IBM DB2 Net Search Extender (NSE), Version 8.1 with IBM DB2 ESE, Version 8.1.
Resource manager	WebSphere Application Server (WAS) Version 4.0.5 Advanced Edition (AE) or Advanced Single Server Edition (AES) or later **For Oracle** JDBC Driver Version 9.0.1

Table 14. Required software for Content Manager servers on AIX (continued)

Component	Required
Resource manager database	**IBM DB2** IBM DB2 UDB Enterprise Edition Version 7.2 or later or IBM DB2 UDB Extended Enterprise Edition Version 7.2.1 and with the Application Development Client for AIX (known as DB2 Software Development Kit, or SDK, in previous versions of DB2) **Or Oracle** Oracle for UNIX Version 8.1.7.4 or later (for Version 8i) or Oracle Version 9.2.0.1 or later (for Version 9i),
Resource manager auxiliary device support	Tivoli Storage Manager API Client Version 4.2.1 (or later) and Tivoli Storage Manager Server Version 4.2.1 (or later) if you want to provide long term storage for your objects on devices other than the fixed disks attached to the resource manager
LDAP	IBM Directory Server 4.1
LUM	IBM License Use Management (LUM) 4.6.2 or later
Information Center browser	Internet Explorer, Version 5 or higher Netscape, Version 4.5, 4.6, or 4.7 **Not compatible:** The Information Center is not compatible with Netscape, Version 6.0 or later

Solaris requirements

Before you install any Content Manager components for Solaris, ensure that your workstation has the correct hardware and software installed. This section lists the required hardware and software for installing and running Content Manager components on Solaris.

Solaris hardware requirements

Table 15. Required hardware for all Solaris components

Component	Required
Server	Solaris SPARC-based processor
RAM	256 MB for each library server 512 MB for each resource manager

Table 15. Required hardware for all Solaris components (continued)

Component	Required
Storage	100 MB combined (for the installed product) of: • The library server • The resource manager 150 MB for the Information Center **Recommended:** • Allow for 300 MB of physical paging space for each server. • Allow for additional hard disk space for data storage.
Display and adapter	VGA (256 color mode)
Other required hardware	• CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations)

Solaris server software requirements

Table 16. Required software for Content Manager servers on Solaris

Component	Required
Operating system	Solaris Version 2.8 or later
Network communication	TCP/IP (installed with Solaris)
Library server compiler	Sun - Forte C++ compiler Enterprise Edition 6 or later

Table 16. Required software for Content Manager servers on Solaris (continued)

Component	Required
Library server database	**IBM DB2** IBM DB2 UDB Enterprise Edition Version 7.2 or later or IBM DB2 UDB Extended Enterprise Edition Version 7.2.1 and with the Application Development Client for AIX (known as DB2 Software Development Kit, or SDK, in previous versions of DB2) **Or Oracle** Oracle for UNIX Version 8.1.7.4 or later (for Version 8i) or Oracle Version 9.2.0.1 or later (for Version 9i), and IBM DB2 UDB Version 8.1, and IBM DB2 UDB Relational Connect Version 8.1 **Optional** If you plan to use the text search feature: • IBM DB2 Text Information Extender (TIE), Version 7.2 with IBM DB2 EE or EEE Version 7.2 • or IBM DB2 Net Search Extender (NSE), Version 8.1 with IBM DB2 ESE, Version 8.1.
Resource manager	WebSphere Application Server (WAS) Version 4.0.5 Advanced Edition (AE) or Advanced Single Server Edition (AES) or later **For Oracle** JDBC Driver Version 9.0.1

Table 16. Required software for Content Manager servers on Solaris (continued)

Component	Required
Resource manager database	**IBM DB2** IBM DB2 UDB Enterprise Edition Version 7.2 or later or IBM DB2 UDB Extended Enterprise Edition Version 7.2.1 and with the Application Development Client for AIX (known as DB2 Software Development Kit, or SDK, in previous versions of DB2) **Or Oracle** Oracle for UNIX Version 8.1.7.4 or later (for Version 8i) or Oracle Version 9.2.0.1 or later (for Version 9i),
Resource manager auxiliary device support	Tivoli Storage Manager API Client Version 4.2.1 (or later) and Tivoli Storage Manager Server Version 4.2.1 (or later) if you want to provide long term storage for your objects on devices other than the fixed disks attached to the resource manager
LDAP	IBM Directory Server 4.1
LUM	IBM License Use Management (LUM) 4.6.2 or later
Information Center browser	Internet Explorer, Version 5 or higher Netscape, Version 4.5, 4.6, or 4.7 **Not compatible:** The Information Center is not compatible with Netscape, Version 6.0 or later

Chapter 7. EIP hardware and software requirements

This section describes hardware and software that are required to install and administer an EIP system.

> **Important**
>
> See the README for the latest version requirements of prerequisite software, including related update or fixpack levels.

Windows requirements

Before you install any EIP components for Windows, ensure that your workstation has the correct hardware and software installed. This section lists the required hardware and software to install before you install the EIP Client, Server or Development Workstation.

EIP client, server and development workstation hardware requirements

When you install EIP on Windows, you must first select one of three machine types: Client, Server, and Development Workstation. The machine type you choose determines which components you can install. See Table 4 on page 47 for a list of the components that you can install with each machine type.

Table 17 describes the hardware required by the Server and Development Workstation machine types. Table 18 on page 68 describes the hardware required for the Client machine type.

Table 19 on page 68 describes the software required by the Server and Development Workstation machine types.

Table 17. Required hardware for EIP Server and Development Workstation machine types

Component	Required
Processor	Intel Pentium 800MHz or equivalent.
RAM	512 MB minimum 1024 MB recommended
Storage	• 1 GB swap space: • 400 MB install space • 10 MB temporary space
Display and adapter	SVGA (800 x 600 resolution and 256 color mode)

Table 17. Required hardware for EIP Server and Development Workstation machine types (continued)

Component	Required
Other required hardware	• Mouse • CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations)

Table 18. Required hardware for EIP client machine type

Component	Specification
Processor	Intel Pentium II 200 MHz minimum Intel Pentium III 400 MHz recommended
RAM	128 MB minimum 256 MB recommended
Storage	• 100 MB swap space: • 210 MB install space • 30 MB temporary space
Display and adapter	SVGA (800 x 600 resolution and 256 color mode)
Other required hardware	• Mouse • CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations)

EIP server and development workstation software requirements

Table 19. Required software for EIP server and development workstation machine types on Windows

Component	Required
Operating system	Microsoft Windows NT 4.0 server with service pack 6 or later, Windows 2000 Server, or Windows XP, or >Net Server 2003 (when available)
Network Communication	TCP/IP installed with Windows

Table 19. Required software for EIP server and development workstation machine types on Windows (continued)

Component	Required
• Administration database • Connector toolkit and samples	• Microsoft Visual C++ Version 6.0 • IBM DB2 Universal Database (DB2 UDB), Enterprise Edition Version 7.2 or later, or • IBM DB2 UDB Enterprise Extended Edition Version 7.2 or later, with DB2 Application Development Client • (Connector toolkit and samples only) Java Development Kit Standard Edition with the latest fixpack • (Optional) IBM DB2 Universal Database Net Search Extender (NSE), (compatible with DB2 Version 8.1) or IBM DB2 Universal Database Text Information Extender (compatible with DB2 Version 7.2). NSE and TIE are only required if you plan to use the text search feature to search a Content Manager Version 8 server.
Federated connector	• IBM DB2 Universal Database (DB2 UDB), Enterprise Edition Version 7.2 or later • Java Development Kit, Version 1.3
Relational Database connector	• IBM DB2 Universal Database (DB2 UDB), Enterprise Edition Version 7.2.1 or later • JDBC driver 1.3 (Java only) • ODBC 3.0 (C++ only) • DataJoiner 2.1.1
Information Catalog connector	• IBM DB2 Universal Database (DB2 UDB), Enterprise Edition Version 7.2.1 or later • JDBC driver 1.3 (Java only) • ODBC 3.0 (C++ only) • DataJoiner 2.1.1
Advanced workflow	• MQSeries Version 5.3.0.2 Server with latest fixpack • MQSeries Workflow Server Version 3.4 or later • Internet Explorer Version 5.0 or later • IBM DB2 Universal Database Version 7.2 or later • For C++, WebSphere MQSeries Version 5.3.0.1 client and MQSeries Workflow V3.4 client are required to run client-side applications. See the MQSeries server and MQSeries workflow documentation for details. **Requirement:** Install the MQSeries Server and MQSeries Workflow software on the machine where you install the administration database. The MQSeries software is required to activate the workflow builder feature, which is installed automatically with the administration database.

Information mining and Web Crawler software requirements

Table 20. Required software for information mining and Web Crawler on Windows

Component	Required
Operating system	Microsoft Windows NT 4.0 with service pack 6 or later, or Windows 2000 Server or Advanced Server
Network Communication	TCP/IP installed with Windows
Information mining	• IBM DB2 Universal Database Version 7.2 plus fixpack 2 or later • Java Runtime Environment (JRE), Version 1.3 or later • DB2 Text Information Extender plus fixpack 2 or later • Federated connector • Java Plug-in Version 1.4.1 or later recommended • WebSphere Application Server Version 4.0.3 with the latest fixpack, or later
Web Crawler	Netscape 5.0 or higher
Web samples for information mining	• WebSphere Application Server (WAS) version 4.0.3 Advanced Edition or Advanced Single Server Edition or later. • Java 2 Software Developer's Kit Standard Edition, Version 1.3, with the latest fixpack.

System administration client hardware requirements

Table 21. Required hardware for the system administration client

Component	Required
Processor	Intel Pentium 800 MHz processor or equivalent
RAM	128 MB
Storage	35 MB for the installed product
Display and adapter	SVGA (1024x768 resolution and 256 color mode)
Other required hardware	• Mouse • CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations)

System administration client software requirements

Table 22. Required software for system administration client

Component	Required
Operating system	Microsoft Windows NT Server Version 4.0, or Microsoft Windows 2000 or Windows XP

Table 22. Required software for system administration client (continued)

Component	Required
Network Communication	TCP/IP installed with Windows
Toolkits	Java Runtime Environment (JRE) 1.3 (included with the program) DB2 Application Development Client Version 7.2 or Version 8.1 (known as DB2 Software Development Kit, or SDK, in previous versions of DB2)

Information Center hardware requirements

Table 23. Required hardware for the Information Center

Component	Required
Storage	150 MB

Information Center software requirements

Table 24. Required software for the Information Center

Component	Required
Browser	Internet Explorer, Version 5 or higher Netscape, Version 4.5, 4.6, or 4.7 **Not compatible:** The Information Center is not compatible with Netscape Version 6.0 or later

AIX requirements

Before you install any EIP components for AIX, ensure that your workstation has the correct hardware and software installed. This section lists the required hardware and software for installing and running Content Manager components on AIX.

AIX hardware requirements

Table 25. Required hardware for all AIX components

Component	Required
Server	RS/6000 based processor
RAM	512 MB
Storage	4 GB for the installed product:
Display and adapter	VGA (256 color mode)

Table 25. Required hardware for all AIX components (continued)

Component	Required
Other required hardware	• CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations)

AIX server software requirements

Table 26. Required software for EIP servers on AIX

Component	Required
Operating system	• AIX 4.3.3 and the latest fix pack (must include TCP/IP and Unicode converter) or AIX 5.1 or later. • Java Developer's Kit/Java Runtime Environment Version 1.3 with fix pack • Java Servlet Developer's Kit Version 2.2, or later • WebSphere 4.0.3, or later
Network communication	TCP/IP (installed with AIX) except standalone topology
Administration database	• IBM VisualAge C++ Version 5 or later • IBM DB2 UDB Extended Enterprise Edition Version 7.2 or later, with the DB2 Application Development Client (known as DB2 Software Development Kit, or SDK, in previous versions of DB2.) • (Optional) IBM DB2 Universal Database Text Information Extender (TIE), Version 7.2 (if you plan to use the text search feature)
Text search client	• C/C++ibmcxx Level 3.6.6.1 or later • Text Search Server Release 6 • Content Manager Version 7.1 connector
Image search client	• C/C++ibmcxx Level 3.6.6.1 or later • Content Manager Version 7.1 connector
Federated connector	• IBM DB2 Universal Database Extended Enterprise Edition Version 7.2 or later, with the Application Development Client for AIX (known as DB2 Software Development Kit, or SDK, in previous versions of DB2.) • Java Software Developer's Kit, Version 1.3

Table 26. Required software for EIP servers on AIX (continued)

Component	**Required**
Relational database connector	• IBM DB2 UDB Extended Enterprise Edition Version 7.2.1 and with the Application Development Client for AIX (known as DB2 Software Development Kit, or SDK, in previous versions of DB2.) Java Database Connect (JDBC) driver Version 1.3 with latest service pack (Java only) • ODBC Version 3.0 (C++ only) • DataJoiner Version 2.1.1
Information catalog connector	IBM DB2 Universal Database Extended Enterprise Edition Version 7.2.1
Administration Workflow	• WebSphere MQSeries Server Version 5.3.0.1 Server with latest fixpack. • MQSeries Workflow Version 3.4 or later • IBM DB2 Universal Database Enteprise Edition Version 7.2.1.
LDAP	IBM Directory server 4.1
Information mining	• IBM DB2 Universal Database Extended Enterprise Edition Version 7.2 with fixpack 2 or later, and with the Application Development Client for AIX (known as DB2 Software Development Kit, or SDK, in previous versions of DB2.) • DB2 Text Information Extender 7.2 plus fixpack 2 or later • Java Runtime Environment (JRE), Version 1.3 or later • Java Plug-in Version 1.4.1 or later • WebSphere Application Server 4.0.3 with the latest fixpack or later • IBM Visual Age C, C++ compiler, Version 5 • IBM Web Crawler
Web samples for information mining	• WebSphere Application Server Advanced Edition or Advanced Single Server Edition 4.0.3 or later, with latest fixpack • Java 2 Software Developer's Kit Standard Edition, Version 1.3, with the latest fixpack.
Information Center browser	Netscape, Version 4.5, 4.6, or 4.7 **Not compatible:** The Information Center is not compatible with Netscape, Version 6.0 or later

Table 26. Required software for EIP servers on AIX (continued)

Component	Required
Connector toolkit and samples	• IBM Visual Age C++ compiler, Version 5 or later for application development using the C++ connector APIs • Java Development Kit, Version 1.3, with latest fixpack

Solaris requirements

Before you install any Content Manager components for Solaris, ensure that your workstation has the correct hardware and software installed. This section lists the required hardware and software for installing and running EIP components on Solaris.

Solaris hardware requirements

Table 27. Required hardware for all Solaris components

Component	Required
Server	Solaris SPARC-based processor
RAM	1 GB
Storage	4 GB for installed product and data storage, depending on workload.
Display and adapter	VGA (256 color mode)
Other required hardware	• CD-ROM drive (for installation only) • Network adapter (if components are installed on multiple workstations)

Solaris server software requirements

Table 28. Required software for EIP components on Solaris

Component	Required
Operating system	Solaris Version 2.8 with patch level SubOS hostname 5.8 Generic_108528-08, or later
Network communication	TCP/IP
Administration database	• IBM DB2 UDB Version 7.2 or later with the Application Development Client. • Sun Forte C and C++ compiler Enterprise Edition 6 update 1 or later

Table 28. Required software for EIP components on Solaris (continued)

Component	Required
Federated connector	• IBM DB2 UDB Extended Enterprise Edition Version 7.2.1 and with the Application Development Client for Solaris. • Sun Forte C and C++ compiler Enterprise Edition 6 update 1 or later • Java Developer's Kit/Java Runtime Environment, Version 1.3.1.2 (IBM version) • Java Plug-ins Version 1.3.1
Relational database connector	• IBM DB2 UDB Extended Enterprise Edition Version 7.2 or later with the Application Development Client. • Java Database Connect (JDBC) driver Version 1.3 (Java only) • ODBC Version 3.0 (C++ only) • DataJoiner Version 2.1.1
Information catalog connector	IBM DB2 UDB Extended Enterprise Edition Version 7.2.1 and with the Application Development Client for Solaris.
Advanced Workflow	• WebSphere MQSeries Server Version 5.3.0.1 Server with latest fixpack • MQSeries Workflow Server Version 3.4 or later • IBM DB2 UDB Enterprise Edition Version 7.2.1 or later
Information mining	• IBM DB2 UDB Extended Enterprise Edition Version 7.2 or later with the Application Development Client. • DB2 Text Information Extender 7.2 plus latest fixpack • Java 2 Runtime Environment Version 1.3, Standard Edition, local or remote • Federated connector • WebSphere Application Server Version 4.0.3 or later with the latest fixpack. • Sun Forte C and C++ compiler, Enterprise Edition 6 • IBM Web Crawler
Web samples for information mining	• WebSphere Application Server (WAS) Advanced Edition, or Advanced Single Server Edition, Version 4.0.3 or later. • Java 2 Software Developer's Kit Standard Edition, Version 1.3, with the latest fixpack.
LDAP	IBM Directory server 4.1
Connector toolkit and samples	Java Developer's Kit/Java Runtime Environment, Version 1.3, with latest fixpack.

Table 28. Required software for EIP components on Solaris (continued)

Component	Required
Text search	• Text Search Server Release 6 • Content Manager Version 7.1 connector
Information Center browser	Netscape, Version 4.5, 4.6, or 4.7 **Not compatible:** The Information Center is not compatible with Netscape, Version 6.0 or later

RMI server requirements

This section describes the operating system requirements to configure an EIP RMI server.

- Windows NT with Service Pack 6, or later
- Windows 2000
- AIX 4.3.4, or AIX 5.1 or later

Client/Server support matrix

Use the matrix in Table 29 to determine the support criteria for connecting EIP connectors, the system administration client, and the Client for Windowst to EIP databases, Content Manager library servers, or to Content Manager resource manager servers.

This matrix is intended to help you to understand the client to server support possibilities. It is also intended to help you to understand how you can upgrade your Content Manager servers from Version 8.1 to Version 8.2 first and then upgrade your clients over time.

Table 29. Client/Server support matrix

	CM Version 8.1 Servers on DB2 Version 7.2 Server +TIE[1]	**CM Version 8.2 Servers on DB2 Version 7.2 Server +TIE[1]**	**CM Version 8.2 Servers on DB2 Version 8.1 Server +NSE[2]**	**CM Version 8.2 Servers on Oracle +NSE[2]**
Version 8.1 CM connector or clients using DB2 Version 7.2 client software	**SUPPORTED**	**SUPPORTED**	**SUPPORTED**	not supported

Table 29. Client/Server support matrix (continued)

	CM Version 8.1 Servers on DB2 Version 7.2 Server +TIE[1]	**CM Version 8.2 Servers on DB2 Version 7.2 Server +TIE[1]**	**CM Version 8.2 Servers on DB2 Version 8.1 Server +NSE[2]**	**CM Version 8.2 Servers on Oracle +NSE[2]**
Version 8.1 CM connector or clients using DB2 Version 8.1 client software	not supported	not supported	not supported	not supported
Version 8.2 CM connector or clients using DB2 Version 7.2 client software	not supported	**SUPPORTED**	**SUPPORTED**	not supported
Version 8.2 CM connector or clients using DB2 Version 8.1 client software	not supported	not supported	**SUPPORTED**	**SUPPORTED**

Notes:

1. Text Information Extender (TIE) - optional for use with Content Manager text search feature with DB2 Version 7.2.
2. Net Search Extender (NSE) - optional for use with Content Manager text search feature with DB2 Version 8.1.

Part 2. Installing Content Manager on a Windows operating system

This section contains information needed to install and configure the IBM Content Manager and Enterprise Information Portal software on the Windows operating system. The information is based on the steps identified using the *Planning Assistant* from the *Start Here CD*.

The prerequisite and installation details in this section are presented in the required order of installation. All steps are presented as if each one is required on this single workstation (for a single server configuration). In fact, you may only need some of the steps, depending on your own configuration needs:

1. Chapter 8, "Installing and updating prerequisite programs for Windows", on page 81
2. Chapter 9, "Performing pre-installation steps on Windows", on page 99
3. Chapter 10, "Installing Content Manager components on Windows", on page 113
4. Chapter 11, "Verifying a successful installation of Content Manager on Windows", on page 153
5. Chapter 12, "Installing Enterprise Information Portal components on Windows", on page 173
6. Chapter 13, "Verifying a successful installation of Enterprise Information Portal on Windows", on page 193
7. Chapter 14, "Installing Content Manager eClient on Windows", on page 201
8. Chapter 15, "Installing the Content Manager Client for Windows", on page 205

Chapter 8. Installing and updating prerequisite programs for Windows

This section has two sub-sections:

1. "Verifying your software prerequisites on Windows" explains how to check the level of a prerequisite that you already have installed on your system.
2. "Installing / Updating Prerequisites" on page 84 has detailed instructions for how to install and configure the prerequisite programs that are needed for your own planned configuration.
   - The steps that you need to perform are determined by the selections that you make while you are using the ″Planning Assistant″ from the *Start Here CD*.
   - The planning assistant produces output sheets (with checklists) for the programs and components that you need to install for your selected components.

   The prerequisite programs included in this section are:
   - "Microsoft Windows Operating System" on page 84
   - "IBM DB2 Universal Database" on page 84
   - "Oracle database on a Windows system" on page 86
   - "IBM DB2 Net Search Extender (NSE) and Text Information Extender (TIE)" on page 90
   - "Microsoft Visual C++ compiler" on page 91
   - "IBM WebSphere Application Server (WAS)" on page 93
   - "Java Development Kit (JDK) Version" on page 95

Verifying your software prerequisites on Windows

Run the following verification checks to determine which of the prerequisites you need to install or update. For those prerequisites that are either not installed or not at the expected level, use the next section ("Installing / Updating Prerequisites" on page 84) to guide you through installing them.

Table 30. Basic prerequisite verification

Prerequisite	How to check	Example value
1. Windows NT SP6 2. Windows 2000 Server SP2	`Winver`	1. Version 4.0 (Build 1381: Service Pack 6) 2. Version 5.0 (Build 2195: Service Pack 2)
Java Development Kit V1.3	`java -fullversion`	Version needs to read 1.3.1 (for example, if you are using the version from WebSphere Application Server, it will read: java full version ″ J2RE 1.3.1 IBM Windows 32 build cn131w-20020403 ORB130″).
UDB EE v7.2 with fixpack 7 or higher	From the DB2 Command Window: `db2level`	Level needs to read ″SQL07025″ or greater with fixpak level of ″WR21306″ or greater.
DB2 UDB Enterprise Server Edition Version 8.1 with fixpack 1	From the DB2 Command Window: `db2level`	Level needs to read SQL08010 or read ″DB2 v8.1.1.27″. The fixpack information needs to read ″FixPak ″1″″ and list the fixpack level. (For example, ″s021124″ is the fixpack that had been available November 24, 2002.) For Oracle, the fixpack level must be S021110 or later.
DB2 Text Information Extender with fixpack 1	From the DB2 command prompt: `db2text start`	1. CTE0185 2. CTE0001 Operation completed successfully

Net Search Extender (required if you use DB2 Version 8.1)	From the DB2 Command Window, start the text search program:
	`db2text start`
	Then type:
	`db2textlevel`
		CTE0350 Instance ″DB2″ uses DB2 Net Search Extender code release ″ tx9_81″ with level identifier ″ tx9_26a″

Table 30. Basic prerequisite verification (continued)

Prerequisite	How to check	Example value
Tivoli Storage Manager API Client Version 4.2.1	`c:\tsm\api\samprun\dapismp`	API Library Version = 4.2.1.0
Tivoli Storage Manager Server Version 4.2.1	Logon to the TSM Server Administration web page: `http://<hostname> :1580` Where `<hostname>` is the name of the TSM server.	The version appears on the Web page. It should say Version 4, Release2, Level1.0
1. WebSphere Application Server AE 4.0.3 2. WebSphere Application Server AES 4.0.3	Check the product.xml file located in: `x:\WebSphere\AppServer\propers\com\ibm\websphere.`	<version>**4.0.3**</version>
Microsoft Visual C++ Compiler Version 6.0	Check **Start --> Programs**.	1. Microsoft Visual C++ 6.0 2. Microsoft Visual Studio 6.0
Microsoft Visual Studio .NET Professional	At the command line, type: `cl`	`Microsoft 32-bit C/C++ Optimizing Compiler Version 13.00.94966 for 80x86 Copyright (C) Microsoft Corporation 1984-2001. All rights reserved.`

Table 31. Prerequisite verification for Oracle

Prerequisite	How to check	Example value
Oracle Version 8.1.7.4 or Version 9.2.0.1 .	Connect to an existing Oracle database: `Squlplus userID/user_password@databasename.domainname` To check the version type: `select * from product_component_version;`	Oracle 8i Enterprise Edition 8.1.7.4.0 PL/SQL 8.1.7.4.0 TNS for 32-bit Windows: 8.1.7.4.0 Oracle 9i Enterprise Edition 9.2.0.1 PL/SQL 9.2.0.1 TNS for 32-bit Windows: 9.2.0.1
DB2 Relational Connect Version 8.1 with fixpack 1	From a DB2 Command Window: `db2level`	Level: s021110 or later

Installing / Updating Prerequisites

The following sections guide you through installing each of the prerequisites, including where you can find download trial versions and fixpacks, how to install them, and how to verify them after installation.

The rule of thumb when installing the prereqs is to always apply the fixpacks after your base components are installed. For instance if you are missing the DB2 UDB Application Development Client from your DB2 install, install this component first, then install the fixpak code. Otherwise you will need to install the fixpak code again after adding any new DB2 pieces.

Microsoft Windows Operating System

One of the following Windows operating systems is required for Content Manager Version 8 Release 2:

- Windows NT with service pack 6, or later, including TCP/IP.
- Windows 2000 Server with service pack 1, or later, including TCP/IP.

Where to obtain Windows service packs

You can download the service packs for the Windows operating systems at the following location:

http://www.microsoft.com/downloads

How to install the Windows service packs

See instructions that come with Windows NT or Windows 2000 product for instructions for installing the service packs.

How to validate that the service pack is installed correctly

From a command prompt, enter the command:

```
winver
```

You should see one of the following:

- For Windows NT: `Version 4.0 (Build 1381: Service Pack 6)`
- For Windows 2000: `Version 5.0 (Build 2195: Service Pack 2)`

IBM DB2 Universal Database

IBM DB2 Universal Database Enterprise Edition Version 7.2 OR Enterprise Extended Edition Version 7.2.1. (or higher) is required for Content Manager Version 8 Release 2. IBM DB2 Universal Database Enterprise Server Edition Version 8.1 (at the fixpack 1 code level) is included in the Content Manager package.

Use this section to install IBM DB2 Universal Database Enterprise Server Edition Version 8.1 with the latest fixpack (included in the Content Manager package) if you are planning to use a DB2 database for your library server and resource manager.

If you are planning to use an Oracle database with your Content Manager library server and resource manager, use the instructions for installing DB2 Universal Database and DB2 Relational Connect that are provided in the section: "Oracle database on a Windows system" on page 86.

Before you begin to install IBM DB2 Universal Database

Before you begin to install IBM DB2 Universal Database:

__ 1. Ensure that your server meets all of the prerequisites and conditions needed to install DB2 Universal Database. To learn more about DB2 prerequisites, insert the DB2 installation CD and click Installation Prerequisites from the DB2 Launchpad.

IBM DB2 Universal Database Enterprise Server Edition, Version 8.1 is provided in the package with the Content Manager software.

__ 2. Make sure that the user ID that you plan to use to install DB2 is a user ID that is part of the ″Administrators″ group, has a local domain, and has the following user rights assigned through the Local Security Policy:

- Act as part of the operating system.
- Create a token object.
- Increase quotas.
- Replace a process level token.

If the domain is not local, the SATCTLDB and DWCTRLDB databases will not be created successfully. If the user does not have the above privileges, the installation will not be able to validate any DB2 usernames.

Refer to Chapter 9, "Performing pre-installation steps on Windows", on page 99, for more information.

Installing IBM DB2 Universal Database

__ 1. Log in to the system with the Administrator account that you have defined for DB2 installation.

__ 2. Close all programs so the installation program can update files as required.

__ 3. Insert the DB2 installation CD-ROM into the drive. If enabled, the auto-run feature automatically starts the DB2 Setup launchpad.

From the IBM DB2 Setup Launchpad (Welcome) window, you can view installation prerequisites and the release notes. You may wan to review the installation prerequisites and release notes for late-breaking information. Click **Install Products** to begin the installation.

When prompted, select Typical as the installation type, to install all DB2 components required to support Content Manager.

__ 4. The DB2 Setup wizard determines the system language, and launch the setup program for that language. If you want to run the setup program in a different language, or the setup program fails to auto start, you can start the DB2Setup wizard manually:

  __ a. Click **Start** and select the **Run** option.

  __ b. In the **Open** field, enter the following command:

  ```
  x:\setup /i language
  ```

  where:

  - x: represents your CD-ROM drive
  - *language* is the territory identifier for your language (for example, EN for English).

  If the /i flag is not specified, the installation program runs in the default language of the operating system.

  __ c. Click **OK**.

__ 5. Once you have initiated the installation, proceed by following the setup program's prompts. Online help is available to guide you through the remaining steps. To invoke the online help, click **Help** or press **F1**. You can click **Cancel** at any time to end the installation. DB2 files will only be copied to your computer once you have clicked **Finish** on the last DB2 Setup wizard installation panel.

For information on errors encountered during installation, see the db2.log file. The db2.log file stores general information and error messages resulting from the install and uninstall activities. By default, the db2.log file is located in the My Documents\DB2LOG\ directory. The location of the My Documents directory will depend on the settings on your computer.

Validating the IBM DB2 Universal Database installation

To validate the DB2 installation:

__ 1. From a DB2 Command Window, enter db2level.

__ 2. You should see the following:

```
DB21085I  Instance "DB2" uses DB2 code release "SQL07025"
(or higher) with level...identifier ...
and informational tokens .... and "WR21306" (or higher).
```

Oracle database on a Windows system

This section helps you set up the required prerequisite programs if you want to access Oracle data sources for your library server. Depending on your planned configuration, you will be installing the following software:

For the library server database component

- Oracle Enterprise server software, Version 8.1.7.4 OR Version 9.2.0.1 or later

- IBM DB2 Universal Database Enterprise Server Edition Version 8.1 with fixpack 1 applied (s021110 or later)
- DB2 Relational Connect Version 8.1 with fixpack 1 applied (s021110 or later)

For the library server application component

If the library server application component is going to be installed on the same machine as the library server database component:

- Oracle Enterprise server software, Version 8.1.7.4 OR Version 9.2.0.1 or later
- IBM DB2 Universal Database Enterprise Server Edition Version 8.1 with fixpack 1 applied (s021110 or later)
- DB2 Relational Connect Version 8.1 with fixpack 1 applied (s021110 or later)

If the library server database component is going to be installed on a remote Oracle server machine from the library server application component:

- Oracle Enterprise client software, Version 8.1.7.4 OR Version 9.2.0.1 or later

Before you begin to install the Oracle server or client software

Before you begin to install IBM DB2 Universal Database, ensure that your machine has enough memory and disk space for the installation, and that you meet all the requirements for the installation. See the following Oracle web site for the platform-specific requirements:

http://technet.oracle.com

Installing the Oracle server software for the library server database component

To install Oracle Enterprise Edition server software, Version 8.1.7.4 OR Version 9.2.0.1 (or later):

__ 1. Log on to the system with a user ID that is part of the ″Administrators″ group.

__ 2. Use the installation procedures in the documentation that comes with the Oracle software for details on how to install the Oracle server software.

Installing the Oracle client software for a remote library server application component

To install Oracle Enterprise Edition client software, Version 8.1.7.4 OR Version 9.2.0.1 (or later):

__ 1. Log on to the system with a user ID that is part of the ″Administrators″ group.

__ 2. Use the installation procedures in the documentation that comes with the Oracle software for details on how to install the Oracle client software. Become aware of any compatibility issues between different levels of Oracle client software and Oracle server software by consulting Oracle documentation, the Oracle TechNet website, the Oracle Metalink website, or Oracle customer service.

__ 3. To ensure that the client software is able to connect to the Oracle server, use the Oracle **sqlplus** tool to connect to an existing database on the Oracle server.

You should see the following fields in your `sqlnet.ora` file in your `ORACLE_HOME/NETWORK/ADMIN` directory:

```
SQLNET.AUTHENTICATION_SERVICES=(NTS)
NAMES.DIRECTORY_PATH= (TSNAMES,ONAMES,HOSTNAME)
```

Before you begin to install IBM DB2 Universal Database

Before you begin to install IBM DB2 Universal Database:

__ 1. Ensure that your server meets all of the prerequisites and conditions needed to install DB2 Universal Database. To learn more about DB2 prerequisites, insert the DB2 installation CD and click Installation Prerequisites from the DB2 Launchpad.

IBM DB2 Universal Database Enterprise Server Edition, Version 8.1 is provided in the package with the Content Manager software.

__ 2. Make sure that the user ID that you plan to use to install DB2 is a user ID that is part of the ″Administrators″ group, has a local domain, and has the following user rights assigned through the Local Security Policy:

- Act as part of the operating system.
- Create a token object.
- Increase quotas.
- Replace a process level token.

If the domain is not local, the SATCTLDB and DWCTRLDB databases will not be created successfully. If the user does not have the above privileges, the installation will not be able to validate any DB2 usernames.

Refer to Chapter 9, “Performing pre-installation steps on Windows”, on page 99, for more information.

Installing IBM DB2 Universal Database Enterprise Server Edition

To Install IBM DB2 Enterprise Server Edition:

__ 1. Insert the DB2 CD and start the setup program—the DB2 Setup Wizard—to install the DB2 server software.

- Insert the CD-ROM into the drive. The auto-run feature automatically starts the DB2 Setup Wizard. If the setup program fails to auto-start, you can start the DB2 Setup Wizard manually.

  To start the DB2 Setup Wizard manually, click Start and select the Run option. In the **Open** field, enter `x:\setup`, where `x:` represents your CD-ROM drive. Then click **OK**.

__ 2. The DB2 Setup Launchpad opens. From this window review the installation prerequisites and release notes for late-breaking setup information.

__ 3. Proceed through the DB2 Setup Wizard installation panels and make your selections.

Installation help is available to guide you through the steps. To invoke the installation help, click **Help** or press F1. You can click **Cancel** at any time to end the installation.

__ 4. Click **Finish** on the last DB2 Setup Wizard installation panel to copy the DB2 files to your system.

When you complete the installation, DB2 is installed in the following directory:

```
\Program Files\IBM\SQLLIB
```

Installing DB2 Universal Database Relational Connect

After you install the client software and the DB2 server software, you need to install DB2 Relational Connect, Version 8 on the DB2 server. DB2 Relational Connect contains the software that you need to access Oracle data sources.

__ 1. Log on to the system with the Administrator account that you have defined for DB2 installation.

__ 2. Close all open programs so that the installation program can update files as required.

__ 3. Insert the DB2 Relational Connect CD into the CD-ROM drive. The auto-run feature automatically starts the setup program. If the setup program fails to auto-start, you can start the setup program manually.

To start the setup program manually, click **Start** and select the **Run** option. In the **Open** field, enter `x:\setup`, where `x:` represents your CD-ROM drive. Then click **OK**.

__ 4. The DB2 Relational Connect Setup Launchpad opens. From this window review the installation prerequisites and release notes for late-breaking setup information.

__ 5. From the Select the features to install panel (in the setup program), choose **Relational Connect for Oracle Data Sources**. The set up will require you to identify the local path where you installed the Oracle client software.

The Relational Connect installation will update the `sqllib/cfg/db2dj.ini` file to set the ORACLE_HOME environment variable.

Caution: If you do not install the Oracle client software before you run the DB2 Relational Connect installation, you will have to manually set the environment variables and link DB2 to the client software.

Installation help is available to guide you through the steps. To invoke the installation help, click **Help** or press F1. You can click **Cancel** at any time to end the installation.

__ 6. As part of the installation:
- Create a DB2 instance on the federated server. This will set the DB2 database manager FEDERATED parameter to YES, which enables the DB2 server to access the data sources.
- Specify the user authorities information for the instance.

__ 7. Click **Finish** on the last setup installation panel to copy the DB2 Relational Connect files to your system.

When you complete the installation, DB2 Relational Connect is installed in the same directory as the DB2 server software.

IBM DB2 Net Search Extender (NSE) and Text Information Extender (TIE)

The powerful text search capabilities of the DB2 Version 7 Text Information Extender (TIE) are merged into the Net Search Extender (NSE) Version 8. Notice that if you plan to use the (optional) text search feature of Content Manager Version 8, you must install:

IBM Text Information Extender (TIE), Version 7.2 with IBM DB2 Enterprise Edition Version 7.2 and Enterprise Extended Edition Version 7.2.1

OR

IBM Net Search Extender (NSE), Version 8 with IBM DB2 Enterprise Server Edition, Version 8.1.

If you are using Oracle as your database application with Content Manager, AND you plan to use the (optional) text search feature of Content Manager, you **must** install NSE, not TIE.

IBM Net Search Extender (NSE), Version 8 is provided in the package with Content Manager, Version 8.2.

Installing IBM DB2 Net Search Extender (NSE) on a Windows operating system

Follow these steps to install DB2 NSE on the Windows operating system:

__ 1. Insert the DB2 Net Search Extender CD into the CD ROM drive

__ 2. Follow the instructions to install NSE. When you get to the window that asks for the user ID and password for the DB2EXT -service, enter the same user name that you specified for your DB2 -service.

Requirements:

- DB2 NSE must be installed on the same workstation as the library server.
- For every DB2 instance, a Windows service is created. Ensure that the *log on as user for DB2 services* is running as this account and not a system account using your Windows user name.

Steps to perform after installing IBM Net Search Extender (NSE)

Update the NSE server configuration file for use with Information Mining:

__ 1. Edit the TIE configuration file `db2extlm.cfg` , in the directory:

```
%DB2HOME%\%DB2INSTANCE%\db2ext
```

__ 2. Increase the default value of the parameter *maxIdxPerDb* to ″100″.

Validating the IBM DB2 NSE installation

To validate the DB2 NSE installation:

__ 1. From a DB2 Command Window, type:

```
db2text start
```

__ 2. You should see information like the following:

```
CTE0185
```

or

```
CTE0001 operation completed successfully
```

Microsoft Visual C++ compiler

Refer to the following website for information about the availability of this product.

http://www.microsoft.com

Installing Microsoft Visual C++

Follow the installation instructions that come with the Microsoft Visual C++ product.

During the installation, look for and make sure that you select **Register environment variables**.

Steps to perform after installing Microsoft Visual C++

Perform the following steps after you install Microsoft Visual C++:

__ 1. Make sure that the Microsoft Visual C++ environment variables are set up correctly:

When Visual C++ is first installed, the environment variables are set up as user variables, not system variables. Therefore, the Visual C++ environment is not automatically available to every user of the library server.

You can change the user environment variables into system environment variables, so that all users have access to the Visual C++ environment.

If you change user variables to system variables, make sure that you place the Visual C++ values after any DB2 or Oracle values.

After you make changes to the environment variables, you must reboot your system to make the variables available to the services.

An example of how to accomplish this task is as follows:

__ a. Logon to the system as the user that installed Visual C++.

__ b. Click **Start** → **Settings** → **Control Panel**.

__ c. Double click the System icon.

__ d. For Windows NT, click the **Environment** tab.

For Windows 2000, click the **Advanced** tab, then click the **Environment Variables** button.

(You can see that the System Variables are above the User Variables for the user that is logged on to the system.)

__ e. Find the **path** variable in the User Variables section of the window and click on it.

(You see that the variable name **path** is displayed in the **Variable:** field. You see the settings of the **path** variable displayed in the **Value:** field of the window.)

__ f. Within this **Value** field, highlight the Microsoft Visual Studio variable, for example:

```
C:\Program Files\Microsoft Visual Studio\Common\Tools\Winnt;
```

__ g. Copy this highlighted information to your clipboard (`CTRL+C`)

__ h. Click on **path** in the System **Variables:** section of the window.

(Now, you see that the information displayed in the **Value** field is the value that is associated with the **path** of the System Variable.)

__ i. Place your cursor in the **Value** field. Scroll to the end of the information field (or after the DB2 values). For example:

```
C:\Program Files\SQLLIB;
```

__ j. Paste (`Ctrl+V`) the information that you copied to your clipboard from the User Variables to this point in the System Variables. (Make sure that there is a semi-colon (;) separating the two variables.)

__ k. Verify that the information is correctly part of the System Variable. If it is correct, then delete the information from the User Variable section. (The C++ variables must be available in the System Variables, and not in the User Variables.)

__ l. Repeat steps 1e on page 92 through 1k on page 92 for both the **lib** variable and the **include** variable.

__ m. Reboot your system to make the variables available to the services.

__ 2. If you install Microsoft Visual Studio Enterprise Edition, the installation may prompt you as to whether to use a new 6.0 database format or to use an older format which is compatible with version 5.0. This format decision has no impact on Content Manager.

Validating the Microsoft Visual C++ installation

To validate the installation, check the **Start --> Programs** menu for either Microsoft Visual C++ 6.0 or Microsoft Visual Studio 6.0.

IBM WebSphere Application Server (WAS)

IBM WebSphere Application Server, Version 5 is provided in this package with Content Manager, Version 8.2. It includes:

- IBM HTTP Server
- Java Development Kit (JDK)

Installing IBM WebSphere Application Server

Be sure your server is configured to meet all of the specific WebSphere Application Server prerequisites and conditions. The WebSphere Information Center contains the prerequisites and conditions and it is located at:

http://www.ibm.com/software/webservers/appserv/library.html

__ 1. Log in to the workstation using the user ID and password that allow you to act as part of the operating system.

__ 2. Insert the WebSphere Application Server CD into the CD drive.

__ 3. Select the language for your locale and click **Next**.

__ 4. Use the LaunchPad to access the product overview, the ReadMe file, and installation guides. Click **Install the product** to launch the installation wizard.

__ 5. The welcome window opens. Click **Next**.

__ 6. The Software License Agreement window opens. Accept the agreement, then click **Next**.

__ 7. When the window opens to Select the type of installation, select **Full** and click **Next**.

__ 8. The window for identifying the directory paths opens. Click **Next** to accept the default destination directories for the WebSphere directory, the IBM HTTP Server directory, and the Embedded Messaging Server and Client directory. Click **Browse** to define a different destination directory for each of the products.

__ 9. In the next window, enter the node name and the host name for this installation. Click **Next**.

__ 10. When the Services window opens, click to check:

- Run WebSphere Application Server as a service
- Run IBM HTTP Server as a service

Enter your user ID and password, then click **Next**.

__ 11. The next window shows you which features have been selected for install. Click **Next**.

__ 12. WebSphere begins copying files to the server.

__ 13. Restart the server after the installation completes.

__ 14. Click **Start** → **Programs** and verify that IBM HTTP Server and WebSphere Application Server AES are listed.

__ 15. Open Services and verify that the IBM HTTP Server and WebSphere Application Server AES are listed as Windows NT or Windows 2000 services.

WebSphere Application Server AES opens and closes multiple command-line interface windows after you restart the workstation. This is a normal part of the installation process.

After you restart the server and the installation program finishes configuring the WebSphere Application Server components, WebSphere Application Server AES automatically launches a First Steps application. First Steps gives you the opportunity to take an interactive tutorial that provides experience with configuring and defining sample data to learn more about the product.

Validating the IBM WebSphere Application Server installation

Follow these steps to validate the IBM WebSphere Application Server installation:

__ 1. Start the WebSphere Application Server.

__ 2. Open **Start->Programs->IBM WebSphere->Application Server V5.0-> Administrator's Console**, and view the information panel under **Help->About**. It should read version 5.0 (or higher).

Another way to validate the installation, is to check the product.xml file:

```
WebSphere\AppServer\properties\com\ibm\websphere
```

It should contain the following information:

```
<version >5.0/version>
```

After installing and validating WAS: verify that the JDBC resource in the Application Server is configured properly. To do this, make sure the WebSphere Application Server is started, then open the Administrator's Console from the Start menu.

__ 1. In the left panel navigate to **WebSphere Administrative Domain->Resources->JDBC Providers**.

__ 2. In the right panel select the **Nodes** tab.

__ 3. Make sure the classpath value for your node is set to **C:\Program Files\SQLLIB\java\db2java.zip**.

Java Development Kit (JDK) Version

JDK, Version 1.3 is required *only* for the following products:

- EIP toolkits.
- Information Mining.
- eClient.
- VideoCharger.
- Installation launchpads.

Where to obtain the Java Development Kit (JDK)

You can use the JDK that comes with WebSphere Application Server. It can be found in the following directory:

```
C:\WebSphere\AppServer\java
```

Since the JDK is part of the WebSphere Application Server, no installation is necessary. However, you **must** ensure that the JDK directory (for example: `C:\Websphere\AppServer\java\bin`) is added to your system path environment variable.

Verifying the correct level of JDK on your system

You can verify that you have the correct level of the Java Development kit as follows:

__ 1. From a command prompt, type: `java -fullversion`.

__ 2. The level should read: `1.3.1`.

If you are using the JDK that comes with WebSphere, it will read:

```
Java full version "J2RE 1.3.0 IBM build cn131w-20020403 ORB130"
```

Installing Workflow for Windows

MQSeries Server has two prerequisites: Active Directory Services Interface (ADSI) 2.0, and Microsoft Management Console 1.1. The MQSeries Server CD includes both products in the `Prereqs` directory. If you are installing on Windows 2000, ADSI and MMC are part of the operating system.

The MQSeries installation CD has an auto-start feature. If you need to install the prerequisites, click **Cancel** when the For Windows - Language Selection window opens and navigate to the Prereqs directory.

Installing MQSeries Server software on Windows

1. If you installed the prerequisites from the MQSeries Server CD, click `Setups/xx_xx/install.exe` where `xx_xx` is the language for your locale. If your workstation configuration already included ADSI 2.0 and MMIC 1.1, insert the CD-ROM labeled **IBM for Windows NT Server** into your CD-ROM drive.
2. If the installation does not start automatically:
   a. Click **Start** ⟶ **Run** from the Windows taskbar.
   b. Enter `x:\setup.exe` in the **Open** field, where `x` is the drive letter for your CD-ROM drive.
   c. Click **OK**.

   The for Windows - Language Selection window opens.
3. Select the language that supports your locale and click **OK**. The Setup window opens, then the Welcome window opens.
4. Click **Next**. The Read License Conditions window opens.
5. Click **Yes** to accept the License Agreement terms.
6. To accept the default installation folders, click **Next**. If you do not want to use the defaults, change them and then click **Next**. The Setup Type window opens.
7. Click **Typical** and then click **Next**. The Set Up Default Configuration window opens.
8. Leave the **Set up a default configuration** check box selected and click **Next**. The Select Options window opens.
9. Leave both check boxes selected in the Select Options window and click **Next**. The Join Default Cluster window opens.
10. Click **Yes, make it the repository for the cluster** and then click **Next**. The Repository Location window opens.
11. Click **Next**. The Select Program Folder window opens.
12. Click **Next**. A folder called **IBM** is added to the Windows **Start** menu under **Programs**. The Ready to Copy Files window opens.
13. Click **Next**. The installation program copies program files to the installation directory. This can take ten or more minutes. The Setup Complete window opens when the installation program finishes copying the files.
14. Click **Finish** to complete the MQSeries server installation process. The service will automatically start as a Windows NT service.

Installing MQSeries Workflow on Windows

After you have installed MQSeries server, you must install MQSeries Workflow to use workflow.

1. Ensure that your workstation meets the prerequisites.

2. Ensure that you have installed MQSeries Server Version 5.2h.
3. Create a temporary folder on your workstation for the MQSeries Workflow installation files; for example, `c:\temp\cmbwf`.
4. Insert the CD in the CD drive.
5. Copy the MQSeries Workflow installation and configuration files from the `WFInstall` directory on the CD to the temporary directory.
6. Open a command window and change to the temporary directory that you created in step 3
7. Remove the CD and insert the MQSeries Workflow CD.
8. If the MQSeries Workflow installation begins automatically, click **Cancel** and **Exit Setup**.
9. To start the MQSeries workflow installation, type: `cmbwfinstall <`*`x`*`> <`*`temp`*`>` where *`x`* is the name of the CD drive and *`temp`* is the name of the temporary directory where you copied the MQSeries Workflow installation and configuration files in step 3 For example, `cmbwfinstall` *`g`*`:` *`c`*`:\`*`temp`*`\cmbwf`.

   To install from a LAN, use the LAN alias instead of the drive letter.
10. Restart the workstation when you see the message `MQSeries Workflow installation completed`.

Configuring MQSeries Workflow on Windows

To configure MQSeries Workflow:

1. Open a command window and change to the temporary directory you created in the previous task.
2. Check the bin subdirectory of the MQSeries Workflow installation is in the PATH.
3. Type cmbwfconfig and wait until the configuration completes. This step creates the default FMC workflow configuration, workflow runtime database, and EIP workflow data container structures. This manual procedure is a one time configuration task.

Starting EIP workflow on Windows

EIP Advanced workflow uses MQSeries Workflow as the underlying workflow engine to deliver workflow functionality. Therefore, starting EIP workflow includes steps to start the MQSeries Workflow.

1. Open cmbupes81.bat in the notepad.
2. Find those two entries which set the EIP administrator user id and password. Modify them according to your custom settings and save the results.

   ```
   @set CMBUPESUSER=icmadmin @set CMBUPESPASS=password
   ```

   The user id and password will be used to start up the EIP collection points monitor (upes) via the `cmbupes81.bat`.

3. Type `cmbwfstart` to start the MQSeries Workflow server and the EIP collection points monitor. Three command windows open. Those three command windows are titled:
   - Trigger Monitor
   - MQSeries Workflow Server
   - IBM MQSeries Workflow PE

The collection points monitor will prompt its startup status in the MQSeries Workflow Server command window. If you choose not to set user id and password in the cmbwfstart.bat, upes will prompt for user id and password when it starts.

Leave those three command windows up while EIP Advanced Workflow is running.

Tip: If you do not require the collection point functionality, enter ’quit’ to shutdown the UPES server. Shutting down the UPES server does not shut down the MQSeries Workflow.

Tip: You need to enable the WorkFlow Service option in the EIP System Administration client before you could define EIP Workflow objects (such as Workflow processes and actions) via the Administration client. After you enable the Workflow Service in the EIP, it is important to keep in mind to have the MQSeries Workflow running when you log on the System Administration client. This is needed to keep the Workflow objects definitions in sync between the EIP Administration database and the MQSeries Workflow runtime database.

Tip: The default MQSeries Workflow system administrator (not configuration administrator) id is ADMIN with default password as ″password″. You would want to change it later for security reason. To do that, first start the MQSeries Workflow and use the fmcautil utilitiy to connect to the Workflow system to change the password. After you have done that, be sure to modify the cmbwfstart.bat to reflect your changes. Here are the steps:

1. `fmcautil ñu admin ñp password`
2. Select `u, p` to change your password and then exit the utility.
3. Update the `CMBWFStart.bat`. For example: `fmcxspea -u=admin -p=myPassword -f`

To configure your MQSeries Workflow server as an RMI server, see Chapter 33, “Configuring an RMI server”, on page 507.

Chapter 9. Performing pre-installation steps on Windows

In addition to installing all the necessary prerequisites, you need to complete the following tasks before installing Content Manager and Enterprise Information Portal:

- "Create user IDs with the proper user rights and privileges"
- "Make sure that you have enough temporary space on your system" on page 101
- "Make sure that your %PATH% is not too long" on page 101
- "Configure Secure Sockets Layer (SSL) for IBM HTTP server" on page 102

Create user IDs with the proper user rights and privileges

Create three user IDs as follows:

- Library server ″administration″ user ID (such as ICMADMIN) if you are installing a library server on this workstation. This user ID **must** be part of the DB2 Admin group.
- ″Database connection″ user ID (such as ICMCONCT) if you are installing a library server on this workstation. (This should be a regular user ID with normal privileges, not part of the DB2 Admin group.)
- Resource manager ″administration″ user ID (such as RMADMIN) if you are installing a resource manager on this workstation. This user ID **must** be part of the DB2 Admin group.

The installation program refers to the IDs by the default names, and you should substitute the names you use if you are not using the default names.

The user ID icmadmin (used for the library server administration) and rmadmin (used for resource manager administration both need to have DB2 Administrative privileges. One simple way to accomplish this is to add icmadmin and rmadmin to the Administrators group. The user ID, icmconct, does not need any special privileges.

In addition, icmadmin and rmadmin need to have the following four user rights:

- Act as part of the operating system
- Create a token object
- Increase quotas
- Replace a process level token

The steps required for assigning these rights differ between Windows NT and Windows 2000:

For Windows NT Operating System:

__ 1. Click **Start -> Programs -> Administrative Tools -> User Manager.**

__ 2. Select **User Rights** from the Policies Menu

__ 3. Enable the **Show Advanced User Rights** checkbox

__ 4. Select the right you want to assign (for example: **Act as part of the Operating System** from the drop-down list of rights

__ 5. Click **Add**

__ 6. Select the user account to the list

__ 7. Click **OK** and **OK** again and then close the User Manager

__ 8. Reboot the server for changes to take effect

For Windows 2000 Operating System:

__ 1. Click **Start -> Settings -> Control Panel**

__ 2. Select **Administrative Tools**

__ 3. Select **Local Security Policy**

__ 4. From the topology tree, select **Local Policies -> User Rights Assignment**

__ 5. Double-click on the right you want to assign (for example: **Act As Part of the Operating System**

__ 6. Click **Add**

__ 7. Select user account from the list

__ 8. Click **OK**

__ 9. The modified user must logoff and log back on for changes to take effect

You need to remember these user IDs and their passwords for entry during the installation. We remind you about them during the installation (at the time that you need to enter them). You can record their names here:

Table 32. Administration and connection IDs

	Default name / information	**Record your value here**
Library server database administration ID	ICMADMIN	
Library server database administration ID password		
Database connection ID	ICMCONCT	

Table 32. Administration and connection IDs (continued)

	Default name / information	Record your value here
Database connection ID password		
Resource manager database administration ID	RMADMIN	
Resource manager database administration ID password		

Make sure that you have enough temporary space on your system

Before installing Content Manager or Enterprise Information Portal, you need to ensure that you have more than 100MB available in the partition where `%TEMP%` is located.

The Content Manager and Enterprise Information Portal installations both use the temporary directory specified in the `%TEMP%` environment variable, (for example: `C:\TEMP` or `C:\WINNT\TEMP`), and they both require about 100MB of free space.

In addition, the Content Manager resource manager installation creates a temporary directory on your `C: partition` and requires about 5MB of free space to be available on your `C: partition`.

Make sure that your %PATH% is not too long

The Content Manager and Enterprise Information Portal installations will append values to your `%PATH%` environment variable. Microsoft Windows limits the length of your path to approximately 1024 characters.

The Content Manager and Enterprise Information Portal installation programs need to add about 100 characters to your path, depending on what you select for your installation directories. One way to verify your `%PATH%` is not too long is by copying it into a word processor and running a word count on it.

If your `%PATH%` is too long, remove duplicate entries first, then you can try to use short names for directories (for example:**Program Files => PROGRA~1**. Use `dir /x` from the command line to look up the short names.

Configure Secure Sockets Layer (SSL) for IBM HTTP server

If you installed WebSphere on this workstation, you need configure Secure Sockets Layer (SSL) for IBM HTTP Server.

This section explains how to configure Secure Sockets Layer (SSL) for IBM HTTP Server on a Windows server to establish secure connections. The resource manager, which requires a web server such as IBM HTTP Server, requires SSL in order to fully communicate with the system administration client. It is important that you follow these instructions very carefully.

Once configured for SSL, you need to enable both http and https access for the resource manager.

See the IBM HTTP Server documentation for the most recent and complete details.

Overview of Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is an encryption system used on servers to ensure that data transferred between a client and a server remains secure and private.

For a server and client to use SSL for secure communications, the server must have two things:

Key pair
A Key pair consists of public and private keys. The keys are used for encryption and decrypting of messages to ensure privacy and confidentiality in transmissions across the internet.

Certificate
The certificates is used for authentication or verification of identity. A certificate can be either self-signed certificate or an issued certificate:

Self-signed
A certificate that you create for your own private Web network

Issued Provided (issued) to you by a *certificate authority* (CA) or by a *certificate signer*.

SSL uses a security handshake to initiate a secure connection between the client and the server. During the handshake, the client and server agree on the keys they will use for the session and the method for encryption. The client authenticates the server using the server certificate.

After the handshake, SSL is used to encrypt and decrypt all of the information in both the HTTPS (a unique protocol that combines SSL and HTTP) request and the server response, including:

- The URL that the client is requesting
- The contents of any form being submitted
- Access authorization information (like user names and passwords)
- All data sent between the client and the server

Configuring secure connections

To have a secure network connection, you will need to complete the following four procedures:

__ 1. Create a new key database (if one does not already exist) and a key.

__ 2. Receive a server certificate from a certificate authority or create a self-signed server certificate using the IBM Key Management Utility (IKEYMAN).

__ 3. Set up SSL using the IBM Administration Server.

__ 4. Test the server installation and configuration.

Creating a new key database

A key database is a file that the server uses to store one or more key pairs and certificates. You can use one key database for all your key pairs and certificates, or create multiple databases. You can create a new key database or you can use an existing key database. If you want to use an existing key database, you can go on to “Creating a self-signed certificate” on page 104.

If you want to create a new key database, continue below.

To create a new key database:

__ 1. Start by creating a folder to store the *keys* database files (for example: C:\keys\). This is a good idea, because the foldermust pre-exist when you actually create the files. You can write the name of the folder here so you can remember it later on in these procedures.

″Keys″ folder (path):	

__ 2. Enter `ikeyman` on a command line or start the Key Management utility in the **IBM HTTP Server** folder (**Start → Programs → IBM HTTP Server → Start Key Management Utility**).

__ 3. Click **Key Database File → New**.

__ 4. In the New window that opens:

   a. Enter your key database name in the **File name** field (for example: **key.kdb**)

   b. Enter the path to the keys folder (that you created in step 1) in the **Location** field

   c. Click **OK**

__ 5. When the Password Prompt window opens:

__ a. Create a password. (A minimum of six characters is required.)

__ b. Confirm the password.

__ c. **Very important:** Select the **Stash the password to a file** check box.

__ d. Click **OK**.

Password Strength guidelines:

You can see the *strength* of the password change by the number of key symbols that appear (up to five keys).You can see five keys appear after you enter a complicated key with mixed-case alpha-numeric characters that include special characters, such as the following example: `MickeyMouse43@#0243`

__ 6. An information window opens to tell you that the password has been encrypted and saved. Click **OK**.

__ 7. Close the IBM Key Management window (**Key Database File ⟶ Exit**).

Creating a self-signed certificate

Use `IKEYMAN` to create a self-signed server certificate to enable SSL sessions between clients and the server. Use this procedure if you are acting as your own CA for a private Web network.

__ 1. Enter `ikeyman` on a command line or start the Key Management utility in the **IBM HTTP Server** folder (**Start ⟶ Programs ⟶ IBM HTTP Server ⟶ Start Key Management Utility**).

__ 2. Click **Key Database File ⟶ Open**.

__ 3. In the Open dialog box, navigate to your key database name (for example: C:\keys\key.kdb), then click **Open**.

__ 4. When the Password Prompt window opens, enter your password (that you created in the previous section) and click **OK**.

__ 5. Select **Personal Certificates** from the dropdown list in the **Key Database content** frame, then click the **New Self-Signed...** button.

__ 6. In the Create New Self-Signed Certificate window, you need to know the following information for these two fields (the other fields are self explanatory):

Key label

Enter a name to identify the key and certificate in the database (for example: **icmrm**). You need to remember this name later when you are setting up to enable SSL.

You can write it in the space on the line below. (You will be reminded to look here when you need to use it again.)

Key label: ____

Common name

Enter the fully qualified host name of the Web server as the common name (for example: www.myserver.com).

Organization

You need to put some information in this field (for example: the name of your company or organization).

__ 7. When you have completed this panel, click **OK**.

__ 8. You can verify that the new Personal Certificate was created successfully and its name appears in the Personal Certificate panel (for example *icmrm).

__ 9. You are now ready to set up SSL using the IBM HTTP administration server.

Close the IBM Key Management window (**Key Database File** → **Exit**).

Setting up SSL using the IBM HTTP Administration Server

Before you begin,

__ 1. Start the following services:

- __ The IBM HTTP Server service
- __ The IBM HTTP Administration service
- __ The Application server (for example WAS AES)

__ 2. Open a browser window on the HTTP server machine and enter the URL http://localhost:8008/admin/ to open the IBM HTTP administration console.

__ 3. Enter your User Name and Password.

Hint If you don't have a User Name and password yet, click the **Cancel** button to get directions for creating them. (Clicking the **Cancel** button actually causes the information page for creating a User Name and password to appear.)

__ 4. After you enter your correct User Name and Password, the Getting Started panel (for the IBM HTTP Server) opens. Wait until the left navigation panel appears (with the title ″IBM Administration Server″), then follow Step 1 through Step 6 below, to configure the SSL.

If you are using the WebSphere Application Server Advanced Edition (AE), you also need to continue with "Additional steps for WebSphere Application Server, Version 4 Advanced Edition (AE)" on page 108.

Step 1: Set up the security module

__ 1. In the left navigation panel, click the arrowhead next to **Basic Settings** (to expand the tree).

__ 2. Select **Module Sequence** (in the tree).

The Module Sequence panel opens with **Scope:** <GLOBAL> shown. (This is the default.)

__ 3. Click the **Add** button (below the list box).

__ 4. Click in the radio button to select **Select a module to add**. Click to expand the drop-down list, then select `ibm_ssl` from the list. The module dll (modules/IBMModuleSSL128.dll) is placed in the field to the right.

__ 5. Click the **Apply** button.

__ 6. Click the **Close** button.

__ 7. Click the **Submit** button.

Step 2: Set up the secure host IP and additional port for the secure server

__ 1. Under **Basic Settings**, click **Advanced Properties** (from the tree).

The Module Sequence window panel opens with **Scope:** <GLOBAL> shown. (This is the default.)

__ 2. Click **Add** for the **Specify additional ports and IP addresses field**.

__ 3. Leave the (optional) IP address field empty, but enter **443** in the **Port** field.

__ 4. Click the **Apply** button.

__ 5. Click the **Close** button.

__ 6. Scroll down to find and click the **Submit** button.

Step 3: Set up the virtual host structure for the secure server

__ 1. In the left navigation panel, click the arrowhead next to **Configuration Structure** (to expand the tree).

__ 2. Click **Create Scope** (in the tree) to open the Create Scope panel.

__ 3. Expand the drop-down list under **Select a valid scope to insert within the scope selected in the right panel** and select **VirtualHost** from the list (default).

__ 4. In the **Enter the virtual host IP address or fully qualified domain name** field, enter the fully qualified host name for the Web server.

__ 5. Enter **443** in the **virtual host port** field.

__ 6. Leave the **Enter the server name** field blank. (This field is used only for redirection URLs. The HTTP Server determines the Server (host) name from its own IP address.)

__ 7. Leave alternate name(s) for host blank.

__ 8. Click the **Submit** button.

Step 4: Set up the virtual host document root for the secure server

__ 1. Under **Basic Settings**, click **Core Settings** (in the tree)

__ 2. Click **Scope**, then select the <Virtual host that you created for SSL> (that was created during the previous step).

__ 3. Again, leave the **Server name** field blank. (This field is used only for redirection URLs. The HTTP Server determines the Server (host) name from its own IP address.)

__ 4. Enter the document root directory name (for example: C:\IBM HTTP Server\htdocs. This is *very important*).

__ 5. Click the **Submit** button.

Step 5: Set keyfile and SSL timeout values for the secure server

__ 1. In the left navigation panel, click the arrowhead next to **Security** (to expand the tree)

__ 2. Click **Server Security** (in the tree) to open the Server Security panel.

Notice that the <Virtual host that you created for SSL> is displayed next to the **Scope** button.

__ 3. Select the **Enable SSL: Yes** radio button.

__ 4. In the **Keyfile filename** field, enter the path and keyfile filename (example: C:\keys\key.kdb)

__ 5. Enter a timeout value for SSL Version 2 session IDs (**100 seconds**).

__ 6. Enter a timeout value for SSL Version 3 session IDs (**1000 seconds**).

__ 7. Click the **Submit** button.

Step 6: Enable SSL and select the mode of Client authentication

__ 1. Under **Security**, click **Host Authorization** (in the tree) to open the Host Authorization panel.

Notice (again) that the <Virtual host that you created for SSL> is displayed next to the **Scope** button.

__ 2. Click to select the **Enable SSL: Yes** radio button. (This enables SSL for virtual secure host.)

__ 3. Click to select the **Mode of client authorization to be used: None** radio button.

__ 4. In the **Server certificate to be used for this virtual host** field, enter the server certificate name that you created during “Creating a self-signed certificate” on page 104(for example: icmrm).

__ 5. Click the **Add** button under the **Cipher specification(s) that can be used in a secure transaction** panel. Add specifications 39, 3A, 62, and 64 by clicking on each one, then clicking the **Apply** button.

__ 6. Click the **Submit** button.

__ 7. Restart the HTTP Server (and leave it open) by clicking on the black circle logo that is located next to the ″help″ **?** in the upper-right corner of the right panel.

Additional steps for WebSphere Application Server, Version 4 Advanced Edition (AE)

If you have WebSphere Application Server Advanced Edition (AE) installed then the Web Server Plugin needs to be generated with SSL information:

__ 1. Make sure that the WebSphere Application Server (WAS) service is started.

__ 2. Invoke the WebSphere Application Administrative Console:

Click **Start --> Programs --> IBM WebSphere --> Application Server AE --> Administrator's Console**

__ 3. Click **Virtual Hosts** in the tree on the left frame of the console Click the **General** tab on the right frame of the console Click **Add**

__ 4. Enter ***:443** in the text area that appears (that's an asterisk, a **colon**, then the numbers 443).

__ 5. Click **Apply**

__ 6. Click **Nodes** (to expand that part of the tree)

__ 7. Right click `<your hostname>` in the tree on the left frame

__ 8. Click **Regen Webserver Plugin**

__ 9. Restart the IBM HTTP Server and the WebSphere Application Server so that the latest plugin information takes effect.

Testing the server installation and configuration

After configuring the Secure Sockets Layer, you should test the server installation with three quick tests. If you don't get the expected results from these tests, you could have a problem with your SSL configuration or you could have a problem with your resource manager installation. If you have a problem, see "Troubleshooting" on page 109.

__ 1. Test of the http connection

__ 2. Test of the https (SSL) connection

__ 3. View your configuration file

To test the http connection:

From a web browser enter the URL:

```
http://your_host/icmrm/snoop
```

You should see the snoop information returned.

To test the https (SSL) connection:

From a web browser enter the URL:

```
https://your_host/icmrm/snoop
```

You should see the snoop information returned here as well.

Special note: The localhost (127.0.0.1) interface will not be enabled for SSL. You must use the external Name to access SSL.)

To view your configuration file and verify your settings:

Navigate to your configuration file (httpd.conf) and view it with a text editor. The bottom of your `httpd.conf` file should look something like the following:

```
LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
Listen 443
LoadModule ibm_app_server_http_module
C:/WebSphere/AppServer/bin/mod_ibm_app_server_http.dll
Alias /IBMWebAS/  "C:/WebSphere/AppServer/web/"
Alias /WSsamples  "C:/WebSphere/AppServer/WSsamples/"
WebSpherePluginConfig C:\WebSphere\AppServer\config\plugin-cfg.xml
<VirtualHost host-name.stl.ibm.com:443>
ServerName host-name
DocumentRoot "c:/ibm http server/htdocs"
ServerAdmin admin@us.ibm.com
ErrorLog "c:/ibm http server/logs/error.log"
TransferLog "c:/ibm http server/logs/error.log"
ServerSignature Off
Keyfile c:\keys\key.kdb
SSLV2Timeout 100
SSLV3Timeout 1000
SSLEnable
SSLClientAuth none
SSLServerCert icmrm
SSLCipherSpec 64
SSLCipherSpec 62
SSLCipherSpec 3A
SSLCipherSpec 39
</VirtualHost>
```

Troubleshooting

Follow the steps in this section to find out why your SSL configuration doesn’t work for your resource manager.

__ 1. Enable logging for the WebSphere Application Server plug-in by changing the trace level from **Error** to **Trace** in the following file:

```
C:\Websphere\AppServer\config\plugin-cfg.xml
```

__ 2. Enable logging for the resource manager by changing the priority of the root component from **INFO** to **DEBUG** and by changing the appender from **ASYNC** to **CONSOLE** in the following file:

```
C:\WebSphere\AppServer\installedApps\<icmrm>.ear
\icmrm.war\icmrm_logging.xml
```

__ 3. Shut down the IBM HTTP Server.

__ 4. Shut down WebSphere Application Server.

__ 5. Delete all the old log files from the folder where you have the WebSphere Application Server logs directed to. The default path for these logs is:

```
C:\Websphere\AppServer\logs
```

__ 6. Restart WebSphere Application Server

__ 7. Check the WebSphere Application Server `stdout.log` and ensure the resource manager connected to DB2. If there is a DB2 connection problem, check for the following conditions in the file listed below:

- __ The `db2java.zip` file is not in the appservers JVM CLASSPATH.
- __ The database name is incorrect
- __ The user name is incorrect
- __ The user password is incorrect

Correct the following file for any indication of the above errors:

```
C:\WebSphere\AppServer\installedApps\<icmrm>.ear
\icmrm.war\WEB-INF\classes\com\ibm\mm\icmrm
\icmrm.properties
```

If you need to change or correct the password, you can enter it in clear text in this file and the server will encrypt it on its first use.

__ 8. Restart IBM HTTP Server.

__ 9. Enter the URL **http://localhost:9080/icmrm/snoop** in Internet Explorer or Netscape.

If the snoop page displays, you have validated that the resource manager snoop servlet is running for normal sockets.

__ 10. Enter the URL **http://your.host.name/icmrm/snoop** in Internet Explorer or Netscape.

If the snoop page displays, you have validated that the resource manager snoop servlet is accessible through the IBM HTTP Server through the normal sockets.

__ 11. Enter the URL **http://localhost:9443/icmrm/snoop** in Internet Explorer or Netscape.

If the snoop page displays, you have validated that the resource manager snoop servlets is accessible through SSL.

If the snoop page does NOT display, the application server is not listening on port 9443. (Port 9443 is used by default by WebSphere Application Server Single Server Edition (AES) with SSL enabled. For WebSphere Application Server Advanced Edition, the port must be configured by hand or you can use a non SSL link for the connection from the IBM HTTP Server plugin to the WebSphere Application Server.)

If this test works, you can choose to modify the resource manager https port to 9443 and not use IBM HTTP Server.

__ 12. Enter the URL **http://your.host.name/icmrm/ICMResourceManager** in Internet Explorer or Netscape.

If a resource manager error panel displays, you have validated that your SSL configuration is working.

__ 13. If, after you have gone through all of these steps, the system administration client still presents an error when it accesses the resource manager, you can have an incorrect password.

You know the following: The password in the icmrm.properties file **is correct** since you are able to access DB2 successfully.

Use the system administration client to change or update the resource manager password in the library server. When you know that the new password is correct and works, login using the new password.

Chapter 10. Installing Content Manager components on Windows

This section is a guide for installing the following Content Manager components on Windows:

- Library server
- Resource manager
- System administration client
- The Information center

Information for installing the other client components are covered later in the following sections:

- Chapter 14, "Installing Content Manager eClient on Windows", on page 201
- Chapter 15, "Installing the Content Manager Client for Windows", on page 205

Before you begin

Before you begin the Content Manager installation:

__ 1. Ensure that you have a user ID that will be used to perform the installation:
   - That is defined locally
   - That belongs to the Local Administrator's group
   - That is one to eight characters in length. **Important:** User IDs must also follow the rules outlined by the relational database manager you are using.

__ 2. If 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
```

   To remove it:

   __ a. Click **Start** → **Settings** → **Control Panel**.

   __ b. Double click the **System** icon.

   __ c. Click the **Environment** tab.

   __ d. Find and delete the `DB2_STPROC_ALLOW_LOCAL_FENCED` variable.

   __ e. **Reboot** your system before you continue with the next step.

__ 3. Know that there are **special instructions** provided for the following required program products:

IBM DB2 Universal Database or Oracle database

Either IBM DB2 Universal Database or Oracle is required for the library server and the resource manager.

If you have not already installed your database application:

- See "IBM DB2 Universal Database" on page 84 for the instructions for installing your DB2 database on the workstation.
- See "Oracle database on a Windows system" on page 86 for instructions for installing your Oracle database on the workstation.

  If the library server application and the library server database will be installed on separate machines:

  a. The library server database **must be created before** the library server application component can be installed.
  b. The library server database on the remote Oracle server must be up and running and have an active Oracle listener associated with it. DB2 will connect to the Oracle database during the library server application installation using the tnsnames and Net8 protocol.

Your database application must be installed **before** you begin the installation of the Content Manager components.

IBM DB2 Universal Database client software

For Oracle/resource manager installations, IBM DB2 client software is required to be installed. (The DB2 JDBC drivers are needed for communication of the resource manager with the library server.)

DB2 Text Information Extender (TIE)

Text Information Extender (TIE) or Net Search Extender (NSE) is required if you plan to use the Text Search feature.

If it is required and you have not installed it, see "IBM DB2 Net Search Extender (NSE) and Text Information Extender (TIE)" on page 90 for instructions to install DB2 TIE or DB2 NSE.

NSE or TIE must be installed on the same workstation as the library server.

IBM WebSphere Application Server (WAS)

IBM WebSphere Application Server is required for the resource manager.

See “IBM WebSphere Application Server (WAS)” on page 93 for instructions for installing and configuring WAS on the workstation. 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.

Important: make sure that you **start** the WebSphere Server Service before you begin the Content Manager installation procedure.

Tivoli Storage Manager
Chapter 30, “Installing and Configuring Tivoli Storage Manager (TSM)”, on page 431 provides the instructions for installing and configuring TSM. TSM is an optional feature that provides long-term storage on devices other than the fixed disks attached to the resource manager. It is installed **after** the resource manager component is installed.

Microsoft Visual C++
Ensure that Microsoft Visual C++ is installed correctly on the workstation where you will install the library server. If you have not already installed it and verified the installation, see “Microsoft Visual C++ compiler” on page 91 for the installation and verification procedure.

__ 4. Ensure that your system meets all of the memory, hardware, and all other software requirements to install Content Manager. Refer to Chapter 6, “Content Manager hardware and software requirements”, on page 55 for a summary of the requirements.

Installing Content Manager on Windows

To start the Content Manager installation program, complete the following steps:

__ 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.)

__ 2. Make sure that you have created the three user ID s that are required for the Content Manager installation process as explained in the section entitled “Create user IDs with the proper user rights and privileges” on page 99.

__ 3. **For Oracle only:** Make the library server user ID that was created during the installation of DB2 a member of the same group as the Oracle user ID. (For example: make the user ID ICMADMIN a part of the *oinstall* group).

__ 4. **For Oracle only:** Grant **Write permission** for the group in the previous step (for example: *oinstall*) to the tnsnames.ora file, located in the directory specified by the Oracle environment variable TNS_ADMIN. During the Content Manager installation process, you will be prompted for the value of TNS_ADMIN. This value must be consistent with the Oracle installation that you intend for use with Content Manager.

__ 5. **For Oracle only:** Verify that the library server database is up and running by logging on to your Oracle client machine:

```
tnsping LS db name.Oracle server domain name
```

If the connection is successful, proceed with the library server application installation. If the connection is not successful, correct the TNS errors reported by Oracle before continuing:

a. Check the tnsnames.ora, listener.ora, and sqlnet.ora files on your Oracle machine for proper configuration.

b. Recycle the Oracle listener on your Oracle server (if necessary) by performing the following steps:

```
lsnrctl stop
lsnrctl start
```

c. Issue the following command to your Oracle server to ensure that your library server database is associated with the active listener:

```
lsnrctl status
```

__ 6. **For Oracle only:** If you experience connectivity problems , for each HOST in the DESCRIPTION section of the tnsnames.ora file, you might need to update the hosts file:

```
/etc/hosts
```

Whether you update this file or not depends on how TCP/IP is configured on your network. Part of the network must translate the remote host name specified in the DESCRIPTION section in the tnsnames.ora file to an address. If your network has a named server that recognizes the host name, you do not need to update the TCP/IP hosts file. Otherwise, you need an entry for the remote host. See your network administrator to determine how your network is configured.

__ 7. Shut down any open Windows applications.

__ 8. Shut down any open DB2 applications, then stop and restart DB2.

__ 9. Start the Content Manager installation by inserting the Content Manager CD into the CD-ROM drive of your workstation. The Content Manager installation launch pad opens and you see ″Welcome to Content Manager″.

- You can click **Prerequisites** to review the install prerequisites (if you have not already done so).

- You can click **Release Notes** to review any ″last minute″ changes or release notes for Content Manager that could apply to your installation.
- You can click **Install Product** to begin the installation of Content Manager.

When you click **Install Product**, the Welcome window opens.

Welcome panel

The first panel (Welcome) of the InstallShield Wizard opens.

Click **Next** to continue the installation.

Software License Agreement panel

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

Click **Next** to continue the installation.

Step 1. Install directory

Choose the directory where the Content Manager program files will be installed:

Table 33. Install location

Install information	Description	Default name / option	Record your value here
Directory name for %icmroot%	Location of the Content Manager program files[1]	C:\Program Files\IBM\CM81	
Directory name for common files	Location of common files that are used by both Content Manager and Enterprise Information Portal	C:\Program Files\IBM\cmgmt	

Note

1. If you have Content Manager and Enterprise Information Portal on the same machine (or plan to install them on the same machine), do not install them to the same directory. If you do, you will have problems in the future if you need to remove or update one of them. (For example: when you remove Content Manager, it can remove common files that you need for Enterprise Information Portal. This problem will not occur if the base programs are each installed in their own directory.)

Click **Next** to continue the installation.

Step 2. Selecting the components to install

The Component Selection window opens, showing you what components are available to install.

Select the components that you want to install. (By default, most components are checked.)

- Click in the box to remove the check mark of the components that you do not want to install.
- Place a check mark in the box for each component that you want to install.

Click **Next** when you are satisfied with your selections.

Depending on the selections that you made on this panel, go to the page indicated in Table 34.

Table 34. Location of next step

Choices	Go to
Library server with IBM DB2 (either alone or with any, or all, of the other components)	"Step LS1. Configure Library Server" on page 119
Library server with Oracle (either alone or with any, or all, of the other components)	"Step ORA1. Select Library Server Components" on page 124
Resource manager with IBM DB2 only (no other components selected)	"Step RM1. Configure Resource Manager Server" on page 121
Resource manager with Oracle only (no other components selected)	"Step ORA2. Select Resource Manager Components" on page 124
Resource manager with IBM DB2 and system administration client	"Step RM1. Configure Resource Manager Server" on page 121
Resource manager with Oracle and system administration client	"Step ORA2. Select Resource Manager Components" on page 124
Resource manager with IBM DB2 and Information center	"Step RM1. Configure Resource Manager Server" on page 121
Resource manager with Oracle and Information center	"Step ORA2. Select Resource Manager Components" on page 124
Resource manager with IBM DB2, system administration client, and Information center	"Step RM1. Configure Resource Manager Server" on page 121
Resource manager with Oracle, system administration client, and Information center	"Step ORA2. Select Resource Manager Components" on page 124

Table 34. Location of next step (continued)

Choices	Go to
System administration client only	"Step SA1. Configure System Administration Client" on page 138
System administration client and Information center	"Step SA1. Configure System Administration Client" on page 138
Information center only	"Step VE1. Verify the install location and component selection" on page 146

Step LS1. Configure Library Server

Skip this step if you are not installing the library server component at this time, and continue with "Step RM1. Configure Resource Manager Server" on page 121.

Enter the following information for your library server database:

Table 35. Library server configuration

Install information	Description	Default name / option	Record your value here
Library server database name	The name of the library server database	ICMNLSDB	
Library server schema name	The library server schema name	ICMADMIN	
Library server database administration ID	Administration ID for the library server[1]	ICMADMIN	
Password (two fields)	Password for the library server administration ID[1]	<password>	
Database connection ID	Database connection ID [2]	ICMCONCT	

Note:

1. This is the Administration ID that you created at the beginning of the install process. See Table 32 on page 100.
2. This is the Connection ID that you created at the beginning of the install process. See Table 32 on page 100.

When you complete your library server configuration, click **Next**.

Program note:

1. At this time the installation program checks to see if a Content Manager (CM) library server database or an Enterprise Information Portal (EIP) system administration database exist on this workstation.

   If a database exists, the program checks to see if it has the same database name, the same user ID, the same schema name, or the same password that you entered.

   - If (only) a CM library server database already exists, the program asks if you want to overwrite the existing database, keep it, or go back to type in new information for the new database.
   - If (only) an EIP system administration database exists, the program asks if you want to share the database between CM and EIP, or if you want to type in another name for the new CM library server database. The installation program cannot create a new separate library server database with the same name as the system administration database. You must give it a different name than the system administration database.
   - If a shared database between CM and EIP already exists, the program asks if you want to proceed with no change to the existing database, or to go back and enter a new information for the database that you want to create.
2. Also, during the time that the library server is being installed, a program called ″library server monitor″ is being created automatically. The library server monitor program's job is to detect the availability of resource managers to a library server database (among other things that are listed in the section called "Running the library server monitor program" on page 498.).

   If the library server monitor program ever stops running abnormally, then you need to restart it by using the procedure that is also described in the section called "Running the library server monitor program" on page 498.

Step LS2. Configure Library Server Options

Select the library server options:

Table 36. Library server configuration options

Install information	Description	Default name / option	Record your value here
Name of library server ID	Enter the name of the library server ID (Range = 1 to 99)	1	

Table 36. Library server configuration options (continued)

Install information	Description	Default name / option	Record your value here
Installation drive (drop-down list of available choices)	The location of your library server database.	C:	
Enable Unicode (check box)	Check this box to enable Unicode.	(not checked)	
Enable text search (check box)	Check this box if you want to use the Text Search feature.[1]	(not checked)	
Note: 1. You must have the DB2 Text Information Extender (TIE) or DB2 Net Search Extender (NSE) installed to use Text Search.			

Click **Next** to continue to the next window.

Step RM1. Configure Resource Manager Server

Skip this step if you are not installing the resource manager component at this time, and continue with "Step SA1. Configure System Administration Client" on page 138.

Enter the identification and authentication information for the resource manager:

Table 37. Configuring the resource manager server

Install information	Description	Default name / option	Record your value here
Resource manager database name	The name of the resource manager database	RMDB	
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>	

Table 37. Configuring the resource manager server (continued)

Install information	Description	Default name / option	Record your value here
Note: 1. This is the Administration ID that you created at the beginning of the install process. See Table 32 on page 100.			

When you complete your resource manager configuration, click **Next**.

Program 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.

Step RM2. Configure Resource Manager Server Options

Enter the information for the resource manager database location, storage drive, and staging area path:

Table 38. Resource manager server options

Install information	Description	Default name / option	Record your value here
Installation drive (drop-down 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 (drop-down list of available choices)	Path to the drive for storing objects for LAN Cache or TSM objects	C:\staging	

Click **Next** to continue to the next window.

Step RM3. Deploy Resource Manager With WebSphere Application Server

Enter the following information to identify the application server that your resource manager will use:

Table 39. Deploying the resource manager

Install information	**Description**	**Default name / option**	**Record your value here**
Application server name [1]	(Optional field)[1] The name of the WAS AE application server	ICMRM	
Web application path	The web path to the WebSphere application server	/icmrm	
Web application name	The name of the Web application	icmrm	
Services port	Enter a port number (the first of five numbers) to be used for resource manager components (migrator, purger, stager, replicator, and asynchronous recovery)	<recommendPort> The recommended port number is displayed on the panel[2].	
Node name	Enter the node name for this resource manager application	<current machine node name>	
WAS administrator user name	Enter the WAS administrator user ID	was_admin	
Password (two fields)	Enter and confirm the password for the WAS Admin user name	<password>	

Note:

1. This is an optional field. It will only be visible in this window if WebSphere Application Server Advanced Edition (AE) is installed on this workstation.
2. You can enter a port number other than the recommended default number. However, it must be the first number of five available contiguous port numbers.

Click **Next** and continue with "Step SA1. Configure System Administration Client" on page 138.

Step ORA1. Select Library Server Components

Skip this step if you are not installing a library server (with Oracle) on this machine.

Select the library server components to install on this machine, and enter the location of the configuration file:

Table 40. Select library server components

Install information	**Description**	**Default name / option**	**Record your value here**
Library server database	Check this box to install the library server database on this machine	(checked)	
Library server application	Check this box to install the library server application on this machine	(checked)	
Location of the default configuration settings file	Path to the default configuration settings file[1]	Default	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.			

Click **Next** to continue.

Step ORA2. Select Resource Manager Components

Skip this step if you are not installing a resource manager (with Oracle) on this machine.

Select the resource manager components to install on this machine, and enter the location of the configuration file:

Table 41. Select resource manager components

Install information	**Description**	**Default name / option**	**Record your value here**
Resource manager database	Check this box to install the resource manager database on this machine	(checked)	

Table 41. Select resource manager components (continued)

Install information	**Description**	**Default name / option**	**Record your value here**
Resource manager application	Check this box to install the resource manager application on this machine	(checked)	
Location of the default configuration settings file	Path to the default configuration settings file[1]	Default	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.

Click **Next** to continue to the next window.

Step ORA3. Configure Oracle Database (1)

Enter the information for the Oracle database server:

Table 42. Oracle server database

Install information	**Description**	**Default name / option**	**Record your value here**
Base directory for Oracle	This is the fully-qualified path under which all Oracle products can be found.[1]	C:\Oracle	
Oracle database server directory	This is the fully-qualified path to your Oracle Enterprise Edition product directory. [1]	C:\Oracle\Ora92	
Oracle TNS Names file location	This is the fully-qualified path to the `tnsnames.ora` file in use for the ORACLE_HOME environment variable.[1]	C:\Oracle\Ora92\network\admin	

Table 42. Oracle server database (continued)

Install information	Description	Default name / option	Record your value here
Oracle NLS message files location	This is equivalent to your ORA_NLS33 environment variable.[1]	C:\Oracle\Ora92\ocommon\nls\admin\data	
Oracle JDBC path	Click **Browse** to find the path to the JDBC directory		
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.			

Click **Next** to continue to the next window.

Step ORA4. Configure Oracle Database (2)

Enter information for the Oracle database server:

Table 43. Oracle database

Install information	Description	Default name / option	Record your value here
Oracle database server version	Select the version of the installed Oracle software[1]	9.2.0.1 OR higher	
Password (two fields)	Enter and confirm the password for the Oracle SYSTEM and SYS user IDs[1]	<password>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.			

Click **Next** to continue and go to the first step indicated by the following questions:

1. Are you installing a library server database or a library server application on this machine?

   If **yes**, go to question 2.

If **no**, go to question 3.

2. Are you installing a library server application on this machine?

   If **yes**, go to "Step OLS1. Configure Library Server Application (1)"

   If **no**, go to "Step OLS6. Configure Library Server Database (1)" on page 130

3. Are you installing a resource manager database on this machine?

   If **yes**, go to "Step ORM1. Configure Resource Manager Database (1)" on page 133

   If **no**, go to "Step ORM5. Configure Resource Manager Application (1)" on page 136

Step OLS1. Configure Library Server Application (1)

Skip this step if you are not installing a library server application on this machine, and go to "Step OLS6. Configure Library Server Database (1)" on page 130.

Enter the information for the library server application to connect to the library server database:

Table 44. Configure library server connections

Install information	Description	Default name / option	Record your value here
Library server database name	Enter the library server database name	ICMNLSDB	
Library server schema name	Enter the library server schema name	ICMADMIN	
Library server database administration ID	This is the user ID that is used to administer your Content Manager library server[1]	oraadmin	
Password (two fields)	Enter and confirm the password	<password>	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.

Click **Next** to continue to the next window.

Step OLS2. Configure Library Server Application (2)

Enter the information for library server database connection ID:

Table 45. Library server connection ID

Install information	Description	Default name / option	Record your value here
Library server database connection ID	Enter the library server database connection ID	ICMCONCT	
DB2 instance owner ID	This is the ID that you created prior to installing the DB2 product.[1]	DB2INST1	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.

Click **Next** to continue to the next window.

Step OLS3. Configure Library Server Application (3)

Enter the information for library server application options:

Table 46. Library server application options

Install information	Description	Default name / option	Record your value here
Library server installation drive	Enter the drive location for the library server	C:\	
DB2 database location	Fully qualified path to the location of the DB2 database that is used with this Oracle database		
Enable unicode	Select to enable unicode	(not checked)	

Click **Next** to continue to the next window.

Step OLS4. Configure Library Server Application (4)

Enter the information for connecting the library server application to the resource manager server:

Table 47. Library server application connection to resource manager

Install information	Description	Default name / option	Record your value here
Resource manager server host name	Enter the resource manager server host name	<hostname>	
Resource manager database administration ID	Enter the resource manager database administration ID	RMADMIN	
Password (two fields)	Enter and confirm the password for the resource manager database administration ID	<password>	

Click **Next** to continue to the next window.

Step OLS5. Configure Library Server Application (5)

Enter more information in this window for connecting the library server application to the resource manager server:

Table 48. Library server application connection to resource manager

Install information	Description	Default name / option	Record your value here
Web application name	Enter the web application name	icmrm	
Web application path	Enter the path for the web application	/icmrm	
Web application port	Enter the port number for the web application	80	
Secure web application port (HTTPS)	Enter the port number for the secure web application	443	

Table 48. Library server application connection to resource manager (continued)

Install information	Description	Default name / option	Record your value here
Token duration (hours)	The amount of time (in hours) that a connection between the library server application and the resource manager can stay active until it is discarded by the system. (Can be modified later with the system administration client tools.)	20	

Click **Next** to continue and go to the first step indicated by the following questions:

1. Are you installing a library server database on this machine?

   If **yes**, go to "Step OLS6. Configure Library Server Database (1)".

   If **no**, go to question 2.

2. Are you installing a resource manager database or a resource manager application on this machine?

   If **yes**, go to question 3.

   If **no**, go to "Step SA1. Configure System Administration Client" on page 138.

3. Are you installing a resource manager database on this machine?

   If **yes**, go to "Step ORM1. Configure Resource Manager Database (1)" on page 133.

   If **no**, go to "Step ORM5. Configure Resource Manager Application (1)" on page 136.

Step OLS6. Configure Library Server Database (1)

Skip this step if you are not installing a library server database on this machine, and go to "Step ORM1. Configure Resource Manager Database (1)" on page 133.

Enter information for the library server database:

Table 49. Library server database

Install information	Description	Default name / option	Record your value here
Library server database name	Enter the library server database name	ICMNLSDB	
Library server database location	Enter the fully-qualified path name of the location where you want Oracle to store its internal database files.[1]		
Library server host name	This is the host-only name of the Oracle server where your library server database is created.[1]	<hostname>	
Library server domain name	This is the domain name that is associated with the host name for the library server (in the row above this one).	<xmpl.name.com>	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.

Click **Next** to continue to the next window.

Step OLS7. Configure Library Server Database (2)

Enter more information for the library server:

Table 50. Library server database (more information)

Install information	Description	Default name / option	Record your value here
Oracle listener name	Enter the name of the Oracle listener[1]	LISTENER	
Oracle protocol	Select the protocol from the drop-down list[1]	TCP/IP	

Table 50. Library server database (more information) (continued)

Install information	Description	Default name / option	Record your value here
Oracle listener port	Enter the port number for the Oracle listener[1]	1521	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.			

Click **Next** to continue to the next window.

Step OLS8. Configure Library Server Database (3)

Enter the authentication information for the library server database:

Table 51. Oracle database administration ID

Install information	Description	Default name / option	Record your value here
Oracle database administration ID	Enter the Oracle database administration ID[1]	oraadmin	
Password (two fields)	Enter and confirm the password for the Oracle database administration ID[1]	<password>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.			

Click **Next** to continue to the next window.

Step OLS9. Configure Library Server Database (4)

Select the configuration options for the library server database:

Table 52. Library server database configuration options

Install information	Description	Default name / option	Record your value here
Enable for unicode	Check this box to enable for unicode	(not checked)	

Table 52. Library server database configuration options (continued)

Install information	Description	Default name / option	Record your value here
Mirror database files	Check this box to mirror database files	(checked)	
Mirror directory	Enter (or browse to) the path for the Mirror directory[1]	C:\Temp	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.

Click **Next** to continue and go to the first step indicated by the following questions:

1. Are you installing a resource manager database or a resource manager application on this machine?

   If **yes**, go to question 2.

   If **no**, go to "Step SA1. Configure System Administration Client" on page 138.

2. Are you installing a resource manager database on this machine?

   If **yes**, go to "Step ORM1. Configure Resource Manager Database (1)".

   If **no**, go to "Step ORM5. Configure Resource Manager Application (1)" on page 136.

Step ORM1. Configure Resource Manager Database (1)

Skip this step if you are not installing a resource manager database on this machine, and go to "Step ORM5. Configure Resource Manager Application (1)" on page 136.

Enter information for the resource manager database:

Table 53. Resource manager database

Install information	Description	Default name / option	Record your value here
Resource manager database name	Enter the resource manager database name	RMDB	

Table 53. Resource manager database (continued)

Install information	Description	Default name / option	Record your value here
Resource manager database location	Enter the fully-qualified path name of the location where you want Oracle to store its internal database files.[1]		
Resource manager host name	This is the host-only name of the Oracle server where your resource manager database is created.[1]	<hostname>	
Resource manager server domain name	This is the domain name that is associated with the host name for the resource manager (in the row above this one).	<xmpl.name.com>	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.

Click **Next** to continue to the next window.

Step ORM2. Configure Resource Manager Database (2)

Enter more information for the resource manager:

Table 54. Resource manager database (more information)

Install information	Description	Default name / option	Record your value here
Oracle listener name	Enter the name of the Oracle listener[1]	LISTENER	
Oracle protocol	Select the protocol from the drop-down list[1]	TCP/IP	
Oracle listener port	Enter the port number for the Oracle listener[1]	1521	

Table 54. Resource manager database (more information) (continued)

Install information	Description	Default name / option	Record your value here
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.			

Click **Next** to continue to the next window.

Step ORM3. Configure Resource Manager Database (3)

Enter the authentication information for the resource manager database:

Table 55. Oracle database administration ID

Install information	Description	Default name / option	Record your value here
Oracle database administration ID	Enter the Oracle database administration ID[1]	RMADMIN	
Password (two fields)	Enter and confirm the password for the Oracle database administration ID[1]	<password>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 147.			

Click **Next** to continue to the next window.

Step ORM4. Configure Resource Manager Database (4)

Select the configuration options for the resource manager database:

Table 56. Resource manager database configuration options

Install information	Description	Default name / option	Record your value here
Mirror database files	Check this box to mirror database files	(checked)	
Mirror directory	Enter (or browse to) the path for the Mirror directory[1]		

Table 56. Resource manager database configuration options (continued)

Install information	Description	Default name / option	Record your value here
Notes: 1. For more information about this field, see “Oracle - expanded information for installation panel fields” on page 147.			

Click **Next** to continue to the next window.

Step ORM5. Configure Resource Manager Application (1)

Skip this step if you are not installing a resource manager application on this machine, and go to “Step SA1. Configure System Administration Client” on page 138.

Enter information for the resource manager application:

Table 57. Resource manager application

Install information	Description	Default name / option	Record your value here
Web application server name	Enter the web application server name	icmrm	
Web application name	Enter the web application name	icmrm	
Web application path	Enter (or browse to) the path for the web application	/icmrm	
Node name	Enter the node name for this resource manager application	<current machine node name>	
WAS administrator user name	Enter the WAS administrator user ID	was_admin	
Password (two fields)	Enter and confirm the password for the WAS Admin user name	<password>	

Click **Next** to continue to the next window.

Step ORM6. Configure Resource Manager Application (2)

Enter information for the resource manager appliction:

Table 58. Resource manager application mount point and staging area

Install information	Description	Default name / option	Record your value here
Mount point	Enter the location of the storage area that is used for storing objects		
Staging area path	Enter the location of the storage area that is used for staging LAN Cache objects or TSM objects		
Resource manager services port	Enter a port number (the first of five numbers) to be used for resource manager components (migrator, purger, stager, replicator, and asynchronous recovery)	<recommendPort> The recommended port number is displayed on the panel[1].	
Note: 1. You can enter a port number other than the recommended default number. However, it must be the first number of five available contiguous prot numbers.			

Click **Next** to continue to the next window.

Step ORM7. Configure Resource Manager Application (3)

Enter information for the resource manager to connect to the library server:

Table 59. Connect the resource manager to the library server

Install information	Description	Default name / option	Record your value here
Library server host name	Enter the library server host name	<hostname>	
Library server database name	Enter the library server database name	ICMNLSDB	

Table 59. Connect the resource manager to the library server (continued)

Install information	Description	Default name / option	Record your value here
Library server schema name	Enter the library server schema name	ICMADMIN	

Click **Next** to continue to the next window.

Step ORM8. Configure Resource Manager Application (4)

Enter additional information for the resource manager to connect to the library server:

Table 60. Library server application administration ID

Install information	Description	Default name / option	Record your value here
Library server application administration ID	Enter the library server application administration ID	oraadmin	
Password (two fields)	Enter and confirm the password for the library server application administration ID	<password>	

Click **Next** to continue to the next window.

Step SA1. Configure System Administration Client

Skip this step if you are not installing the system administration client component at this time, and continue with "Step CNLS1. Connect Library Server To Resource Manager" on page 141.

Enter the appropriate information into the following fields to configure your system administration client:

Table 61. System administration client configuration

Install information	Description	Default name / option	Record your value here
Library server database name	The name of the library server	ICMNLSDB	
Library server schema name	The library server schema name	ICMADMIN	

Table 61. System administration client configuration (continued)

Install information	Description	Default name / option	Record your value here
Authentication type	Related to DB2 database manager authentication[1]: Choose **Client** or **Server** to match the settings on your DB2 server.	Server	
Database connection ID	Enter the database connection ID[2]	ICMCONCT	
Password	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. If you are not sure which option to choose, contact your DB2 administrator.
2. This is the Connection ID that you created at the beginning of the install process. See Table 32 on page 100. The database connection ID and password areas are enabled for the **Server** option only. They are disabled if you choose the **Client** option.
3. The Enable single sign on option is enabled only if you selected the **Client** option. It is disabled if you choose the **Server** option.

When you have completed your system administration client configuration, click **Next**.

Step SA2. Define Location Of System Configuration Information

During this step you indicate where your system configuration information is located for this system. Because of the flexibility of Content Manager, you have a number of options:

1. 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.)
2. You can use system configuration information on an HTTP web server.

3. 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).
4. You can use a combination of any of the above three options.

   You can use any one of the above options (1, 2, or 3)

   OR

   You can use two of the options

   OR

   You can use all three of the 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.

Enter the information as follows:

Table 62. System configuration information

Install information	Description	Default name / option	Record your value here
Select **Local** or **Remote**	Select **Local** to install the configuration information on this workstation. Select **Remote** if your configuration information is located (or will be located) on a remote, network-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>	
Web Server	Area for entering a valid URL address (in the form http://...) of the remote web server	(no default)	

Table 62. System configuration information (continued)

Install information	Description	Default name / option	Record your value here
Enable LDAP (check box)	Check this box if you would like to use datasources configuration information stored on an LDAP server.	(not checked/no)	

Click **Next** to continue to the next window.

Step CNLS1. Connect Library Server To Resource Manager

Skip this step if any one of the conditions listed in Table 63 are true, and continue with the step indicated. Otherwise, continue below.

Table 63. Location of next step

Condition	Continue with (go to)
If you are not installing a library server or a resource manager at this time	"Step VE1. Verify the install location and component selection" on page 146
If you are installing a resource manager, **but not** a library server at this time	"Step CNRM. Connect Resource Manager To Library Server" on page 143

Enter the information about the resource manager that the library server needs to connect to it:

Table 64. Connect library server to resource manager

Install information	Description	Default name / option	Record your value here
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 for the Web Application Server	80	

Table 64. Connect library server to resource manager (continued)

Install information	Description	Default name / option	Record your value here
Secure Web application port (HTTPS)	Port number for the resource manager to communicate with the system administration client	443	
Web application path	Same as the path entered in "Step RM3. Deploy Resource Manager With WebSphere Application Server" on page 122	/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>	
Token duration (hours)	The amount of time (in hours) that a connection between the library server and the resource manager can stay active until it is discarded by the system. (Can be modified later with the system administration client tools.)	48	

Click **Next** to continue to the next window.

Step CNLS2. Connect Library Server To Resource Manager Part 2

Skip this step if the library server and the resource manager are being installed on the same machine.

Enter the resource manager database connection ID and password:

Table 65. Resource manager connection ID

Install information	Description	Default name / option	Record your value here
Resource manager database administration ID	See Note 1 (below).	RMADMIN	
Password (two fields)	See Note 1 (below).	<password>	
Note: 1. These are the same values that were entered during "Step RM1. Configure Resource Manager Server" on page 121.			

Click **Next** to continue to the next window.

Step CNRM. Connect Resource Manager To Library Server

Skip this step if you are not installing a resource manager at this time, or if you are installing both a library server and a resource manager on this same machine.

Enter the information about the library server that the resource manager needs to connect to it:

Table 66. Connect resource manager to library server

Install information	Description	Default name / option	Record your value here
Library server host name	The host name of the workstation that contains the library server	<host name>	
Library server database name	See Note 1 (below).	ICMNLSDB	
Library server schema name	See Note 1 (below).	ICMADMIN	
Library server database administration ID	See Note 1 (below).	ICMADMIN	
Password (two fields)	See Note 1 (below).	<password>	

Table 66. Connect resource manager to library server (continued)

Install information	Description	Default name / option	Record your value here
Note: 1. These are the same values that were entered during "Step LS1. Configure Library Server" on page 119.			

Click **Next** to continue to the next window.

Step LDAP1. Configure components for LDAP

Select the components that you want to enable for LDAP:

Table 67. Enable LDAP options

Install information	Description	Default name / option	Record your value here
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[1]	(not checked/No)	
Resource manager server (check box)	Check this box to allow user authentication for the resource manager by an LDAP server	(not checked/No)	
Note: 1. If you check the system administration client (to allow importing of users from an LDAP server), and if you are installing a library server on this machine, it is a good idea to also check the library server check box (to allow user authentication for the library server).			

Click **Next** to continue to the next window.

Step LDAP2. Define LDAP Server

Skip this step if you did not select any of the options on the previous panel to enable LDAP, and go to “Step VE1. Verify the install location and component selection” on page 146.

Enter the information for the LDAP server that you want to use:

Table 68. Define the LDAP server

Install information	Description	Default name / option	Record your value here
LDAP server type (drop-down list of available choices)	Select either **Standard LDAP**[1] or **Active Directory** from the drop-down list	Standard LDAP	
Host name	Enter the host name of the LDAP server machine	ldap:// ldapServer.ibm.com	
Port	Enter the port number on the LDAP server machine	389	
LDAP server administration ID	Enter the LDAP server administration ID for LDAP on the LDAP server machine	cn = root (default for IBM Directory) <adminId> (default for Active Directory)	
Password	Enter the password for the LDAP server administration ID	<password>	
Note: 1. Select Standard LDAP for IBM Directory or for Domino NAB.			

Click **Next** to continue to the next window.

Step LDAP3. Configure LDAP Server

Enter configuration information for the LDAP server

Table 69. Configure the LDAP server

Install information	Description	Default name / option	Record your value here
Base distinguished name	Refer to the LDAP documentation for information about the base distinguished name	o=ibm, c=US	
User authentication attribute	Refer to the LDAP documentation for information about the user authentication attribute	cn	
Search scope	During search operations against an LDAP, search at one level or in a subtree fashion[1]	Subtree	
Referral	Choose to **Ignore** or **Follow** a reference to another LDAP server[1]	Ignore	
Note: 1. See the LDAP documentation for more information			

Click **Next**, and continue to the next step.

Step VE1. Verify the install location and component selection

Verify that the installation information is correct. If any parameters are incorrect, you can return to previous windows by using the **Back** buttons. Click **Next** to complete the installation.

The Content Manager install program goes to work

The Start Copying Files window opens.

You will see a message that installation has been successful. Click **Finish**.

If you received a message during installation, you can view it in the `log.txt` file in your `%ICMROOT%` directory. (Where `%ICMROOT%` is the directory where Content Manager is installed.)

First steps - verify the installation

After the installation of a Content Manager system administration client, the First Steps launchpad appears. You can use it at that time, or you can come back to it at any time by pressing **Start → IBM IBM Content Manager for Multiplatforms V8.2 → First Steps**.

The First Steps window opens:

1. Click **View First Steps information** to read the introduction to the First Steps process.
2. Click **Load Sample Data** to store the samples into the Content Manager database.
3. Click **Work with Sample Data**. The system administration client opens. You can use it to see how Content Manager makes use of the new data model to manage objects. Some examples of what you can do are as follows:
   a. You can open the item type Policy and go to the Attributes page:
      - Attributes and attribute groups appear to the left
      - You can see that Policy is the name of the item type
      - Insured and VIN are child components of Policy
      - Address is an attribute group
      - Policy_Number shows you an attribute that is free of a child component or an attribute group
   b. You can explore the sample data for each object
   c. You can create your own objects and add them to the sample data
   d. You can delete users and re-create them

You can refer to the system administration client's online help for assistance on specific tasks.

Oracle - expanded information for installation panel fields

This section is provided to give more detail for the information that is added to specific fields during the installation.

Location of the default configuration settings file

You can re-use an existing `icmlsdb.properties` for the library server (or `icmrmdb.properties` file for the resource manager) file as input to the installation process. If no path is provided, values from a default version of the file will be used by install. You can modify or accept these values during the course of the installation. It is also possible to have a custom-made `icmlsdb.properties` file for the library server (or `icmrmdb.properties` file for the resource manager) for use in deploying a new library server (or Resource Manager). However, this is not recommended due to the importance of the accuracy of the information in the `icmlsdb.properties` for the library server (or `icmrmdb.properties` file for the resource manager) file.

Base directory for Oracle

This is the fully-qualified path under which all Oracle products can be found. During your initial installation of the Oracle product, you were asked for this value during Oracle product installation. This is the ORACLE_BASE environment variable. For example, if you have installed both Oracle Enterprise Edition and the Oracle Universal Installer, you might have a directory tree similar to the following:

```
/opt/oracle/  ---> /opt/oracle/product/8.1.7
                 |
                  --> /opt/oracle/oui
```

In this example, `/opt/oracle` would be the value of your `ORACLE_BASE` environment variable.

Oracle database server directory

This is the fully-qualified path to your Oracle Enterprise Edition product directory. Under this directory is the Oracle `database bin`, `network`, `dbs`, and other related directories. This is equivalent to your `ORACLE_HOME` environment variable. In the example above, the `ORACLE_HOME` value would be `/opt/oracle/product/8.1.7`

Oracle TNS Names file location

This is the fully-qualified path to the `tnsnames.ora` file in use for the `ORACLE_HOME` environment variable that you specified in the previous step. The value for this field is equivalent to your Oracle `TNS_ADMIN` environment variable. The oracle user ID should have full access to this `TNS_ADMIN` location. Additionally, this file must have write permissions for the Oracle group so that the db2 instance user ID (which must also be a member of the Oracle group) can update the information for Content Manager.

Oracle NLS message files location

For most customers, this value should be `ORACLE_HOME/ocommon/nls/admin/data`. It is equivalent to your Oracle `ORA_NLS33` environment variable. This setting is intended primarily for customers who have different installations of Oracle on the same machine and utilize different language versions.

Oracle database server version

If you are using any version of Oracle 9.2.0.1 or higher, you should select ″9.2.0.1 or higher″. If you are selecting any version of Oracle 8.1.7.4 or higher, but are not using Oracle 9i, you should select ″8.1.7.4 or higher″. Note that Content Manager does not support Oracle versions of 9i less than 9.2.0.1, nor any versions of 8i less than 8.1.7.4.

Refer to Oracle’s Metalink website for any patchsets and related installation instructions you may need to upgrade your Oracle system prior to installing Content Manager.

Password (for Oracle SYS and SYSTEM)
This is the password that will be *set* for the Oracle-created accounts SYS and SYSTEM. At database creation time, these two internal accounts are set with the password value you provide here. As indicated in Oracle security guidelines, you should differentiate the password used for these accounts after database creation. Setting the passwords provides additional security for the administration of your Oracle database.

Library server database administration ID/Schema name
This will be the user ID used to administer your Content Manager library server. In most cases, this will also be your Library server schema name. Therefore, unless you specifically want to have your library server schema ID separate from your library server administrator ID, these two values will be the same (for example: `icmadmin`).

DB2 instance owner ID
This is the user ID you created prior to installation of the DB2 product. It is the user ID that you specified during installation of DB2 as the DB2 instance user ID. It is also the user ID that you included in the Oracle user ID group. As the user ID that owns a DB2 instance, this user ID, by default, also has `DB2 SYSADM` privileges which are needed to create a DB2 federated database that connects to your Oracle data source.

Library server database location
This should be the fully-qualified path name of the location where you want Oracle to store its internal database files. Additionally, this directory will be used by the installation program to generate intermediate files and database creation log files. It keeps a copy of your `icmlsdb.properties` file for future use. If you will be installing the library server application on an Oracle client machine, you should use `ftp` to connect to this file to your Oracle client machine (to save time and provide default values for the library server application installation). If the directory provided in this field does not exist, the installation program creates it for you. If you are using a directory that already exists, you must ensure that it is owned by the Oracle user ID and has write permissions for the Oracle user ID and Oracle group.

Library server host name
This is the host-only name of the Oracle server on which your library server database will be created. If you are installing a library server

database, this will be the host name for the local Oracle server machine. If you are installing the library server application, this will be the host name for the Oracle server machine that *already* contains your library server database.

Oracle listener name

For most Oracle installations, and the value provided by default during an Oracle installation, you will never need to specify a value other than `LISTENER`. If, however, you are certain that your organization uses named listeners and you want to use a specific listener, please enter that name in this field. You can check to see the name of the current, active listener on your Oracle server by issuing the following command:

```
lsnrctl status
```

If the active listener is not the listener you wish to use, you can check your `listener.ora` file on the Oracle server to determine which available, named listener you wish to use. If you want to create a new listener, the listener must be added to your `listener.ora` file before beginning Content Manager installation.

For proper operation of Content Manager, the listener name you specify in this field must be the active listener on your Oracle server at all times.

Oracle protocol

In most cases, you should accept the default value of `TCP/IP` for the Oracle communications protocol to be used. If you choose to select another Oracle-supported protocol, you must verify that your Oracle client/server environment is correctly configured for this protocol using the Oracle `TNSNAMES` naming method and the Oracle Net8 database communications protocol.

Oracle listener port

Most Oracle installations use a default listener port of 1521. If you know that the named listener you wish to use has a different protocol, please specify that value here. You can verify this by referring to your Oracle `listener.ora` file.

Oracle database administration ID

To maximize the security of your library server database and Oracle system, it is good practice to choose a different value for this field than the user ID and password that you provide for the library server administrator user ID and password. This user ID owns the Oracle database and tables and is created as an internal Oracle user only. DB2 Relational Connect does not support the use of other Oracle external authentication methods. Therefore, this user ID MUST remain an internal, Oracle-authenticated user ID. Users can change the Oracle user ID associated with the library server database after installation by running the Content Manager user mapping utility, `icmsumap` for Sun platforms. However, you must ensure that the new user ID has identical Oracle permissions to the previous user ID in use. You should not change this value once Content Manager has been installed, but instead change only the password associated with the user, unless your organization's security policy dictates otherwise.

Password (for Oracle database administration ID)

This value should not be the same value used for your library server administrator password. This is to maximize the security of your library server database and Oracle system.

Mirror directory

If you choose to use this Oracle mirroring option, it enables Oracle to mirror the Oracle log files (useful for recovery purposes). Refer to your Oracle server documentation for more information about mirroring.

Resource manager database location

This should be the fully-qualified path name of the location where you want Oracle to store its internal database files. Additionally, this directory will be used by the installation program to generate intermediate files and database creation log files. It keeps a copy of your `icmrmdb.properties` file for future use. If you will be installing the resource manager application on an Oracle client machine, you should use `ftp` to connect to this file to your Oracle client machine (to save time and provide default values for the library server application installation). If the directory provided in this field does not exist, the installation program creates it for you. If you are using a directory that already exists, you must ensure that it is owned by the Oracle user ID and has write permissions for the Oracle user ID and Oracle group.

Resource manager host name

This is the host-only name of the Oracle server on which your resource manager database will be created. If you are installing a resource manager database, this will be the host name for the local Oracle server machine. If you are installing the resource manager application, this will be the host name for the Oracle server machine that *already* contains your resource manager database.

Chapter 11. Verifying a successful installation of Content Manager on Windows

Use information in this section to verify a successful installation of Content Manager on a Windows system:

“Verify library server database”

“Verify library server access modules generated” on page 154

“Verify that the library server monitor program is running” on page 155

“Verify resource manager deployment” on page 155

“Verify resource manager Web application in a Web browser” on page 156

“Verify resource manager database” on page 156

“Verify the installation by running Content Manager First Steps” on page 157

Verify library server database

To verify that the library server is installed correctly:

__ 1. Open a DB2 command window (**Start -> Programs -> DB2 -> Command Window**)

__ 2. Check database connection by typing:

```
db2 connect to <icmnlsdb> user <icmadmin> using <password>
```

You should see output similar to the following:

```
Database Connection Information
Database server        = DB2/NT 7.2.0
SQL authorization ID   = ICMADMIN
Local database alias   = ICMNLSDB
```

__ 3. Check database tables by typing:

```
db2 list tables
```

You should see several tables listed (around 100); some with names starting with ″FA″ (29 tables) and some starting with ″ICM″ (109 tables). For Oracle: you will not see any tables with names starting with ″FA″. You will only see tables with names starting with ″ICM″.

__ 4. You can also check `%ICMROOT%\logs\icmcrlsdb.log` and search for the term `SQLSTATE=` to find error messages. A few of the `SQLSTATE` messages are normal and you need to read the surrounding text to determine if there may have been a problem. For example, you should expect to find `SQLSTATE=08003` messages in the log after the `CONNECT RESET` commands.

For Oracle only: Log files generated during Oracle database creation will be in the ″Library server database location″ specified during install, ending with the suffix `.log`. Log files generated during DB2 database creation will be in the `%TMP% directory`, `icmlscrdb.db2.log`.

If database creation fails, you should verify the values used in your `icmlsdb.properties` file. For Oracle database creation, this file will be located in the ″Library server database location″ specified during installation. For DB2 database creation, this file will be located in the `%TMP% directory`. If one of the values in the properties file is incorrect, you can edit the file to correct the value. Once you are satisfied that the properties file is correct, re-run the installation program and browse to the directory where their properties file is located. You should also verify your `tnsnames.ora`, `listener.ora`, and `sqlnet.ora` on your Oracle server using the methods already described. The `sqlnet.ora` file on the Oracle client machine should use the same settings described earlier for the Oracle server.

Verify library server access modules generated

The access modules are used for CM item types. They are dynamically generated using the C++ compiler.

Look for .dll files in `%ICMROOT%\<db name>\dll`. If you are using a shared database with EIP, the dlls may be located at `%CMBROOT%\<db name>\dll` instead. (This does not apply for Oracle installations).

Troubleshooting

__ 1. If the dlls are not there, then your compiler environment settings may not be set up correctly for CM. You may find some .tx3 files in the `<db name>\dll` directory instead which will contain error messages.

__ 2. Verify that you have *moved* (not copied) the Microsoft C++ environment variables from USER variables to SYSTEM variables. See “Microsoft Visual C++ compiler” on page 91 for more information.

__ 3. If you did not register the C++ environment variables during the compiler installation, you can try to do it manually by looking inside `Microsoft Visual Studio\VC98\bin\vcvars32.bat` at the location where you have installed the compiler. You can use `vcvars32.bat` to determine what you should set your environment to.

__ 4. **For Oracle only:** In the INCLUDE, LIB, and PATH variables, make sure that DB2 information appears before any Oracle information.

Verify that the library server monitor program is running

To verify that the library server monitor is running, use the procedure for "Running the library server monitor program" on page 498.

Verify resource manager deployment

To verify that the resource manager deployed correctly:

__ 1. Check that the <icmrm> web application and ICM_Server web application server are listed. Note that icmrm is the default name and will be different if you changed it during the install

  __ a. Open the Administrative Console from **Start -> Programs -> IBM WebSphere Application Server AE(s) V4.0 -> Administrator's Console.**

  __ b. Select **Open a configuration file to edit with the console**

  __ c. Select the option - **Enter full path to file on server** - and enter the path to the `IDM_ICM.xml` configuration file located in your Content Manager Common directory (e.g. `C:\Program Files\IBM\CMgmt`)

  __ d. On the left-hand topology pane, expand

```
+ WebSphere Administrative Domain
             + Nodes
                  +<hostname>
                        +Application Servers
```

  to find the ICM_Server application server.

  __ e. Expand

```
+WebSphere Administrative Domain
            +Nodes
                +<hostname>
                     +Enterprise applications
```

  to find the <icmrm> web application.

You should see the icmrm application server started. You should also see the icmrm web application.

If this validation fails, your resource manager did not deploy correctly and you will have to manually deploy the ICMRM Web application. Instructions on how to do this on WAS AE can be found in "Deploying and configuring the resource manager with WAS Advanced Edition (AE)" on page 496.

__ 2. Open a DB2 command window (**Start -> Programs -> DB2 -> Command Window**). Check RM processes are running by typing:

```
db2 list applications
```

You should see output similar to the following:

```
Auth Id Application Appl.  Application Id           DB     # of
Name    Handle                                      Name   Agents
------- ----------- ----- ------------------------ -------- ------
RMADMIN  java.exe    23   *LOCAL.DB2.020625001135    RMDB     1
RMADMIN  java.exe    24   *LOCAL.DB2.020625001136    RMDB     1
RMADMIN  java.exe    25   *LOCAL.DB2.020625001137    RMDB     1
```

The three java.exe processes are related to RMDB

__ 3. You can also check to see if the icmrm files have been copied to the WAS directory, for example:

```
C:\WebSphere\AppServer\installedApps\icmrm.ear\
```

Verify resource manager Web application in a Web browser

To verify the resource manager Web application in a Web browser:

__ 1. Start your WebSphere Application Server if it is not already started.

For WAS AE
Start the IBM WS AdminServer 4.0 from the Services panel.

For WAS AES
Start the IBM WS Admin Server by running `IDM_ICM_Start.bat` located in the CM installation directory (e.g. `C:\Program Files\IBM\CM81`)

__ 2. Open a web browser and type in the following web addresses:

http://<hostname>/icmrm/snoop

You should see the snoop information returned using http which should display network settings for your machine.

__ 3. Now, enter the following web address for your secure (SSL) connection:

https://<hostname>/icmrm/snoop

You should see the snoop information again using https which will test your SSL connection.

More information about the SSL configuration is in the section “Configure Secure Sockets Layer (SSL) for IBM HTTP server” on page 102.

Verify resource manager database

You can verify that the resource manager database is installed correctly as follows:

__ 1. Open a DB2 command window (**Start -> Programs -> DB2 -> Command Window**):

__ 2. Check database connection by typing:

```
db2 connect to <rmdb> user <rmadmin> using <password>
```

You should see output similar to the following:

```
Database Connection Information

Database server        = DB2/NT 7.2.0
SQL authorization ID   = RMADMIN
Local database alias   = RMDB
```

__ 3. Check database tables by typing:

```
db2 list tables
```

You should see numerous tables listed

__ 4. You can also check `%ICMROOT%\logs\icmcrrmdb.log` and search for the term `SQLSTATE=` to find error messages.

A few of the SQLSTATE messages are normal and you need to read the surrounding text to determine if there may have been a problem. For example, you should expect to find `SQLSTATE=08003` messages in the log after the CONNECT RESET commands.

Verify the installation by running Content Manager First Steps

Content Manager First Steps allows you to load sample data into the Content Manager servers. You perform the First Steps procedures differently depending whether you have all of the Content Manager components on one system or if you have them installed on more than one system.

If you have all of the Content Manager components on one system, begin the first steps process in the section: "Running First Steps for a single Windows machine Content Manager system"

If you installed the Content Manager library server, and/or your resource manager on another machine from your system administration client, use the procedures for First Steps in the section: "Running First Steps for a multiple machine Content Manager system" on page 158

Running First Steps for a single Windows machine Content Manager system

Start the first steps here if you installed all of the Content Manager components on a single Windows operating system machine:

__ 1. Click **Start -> Programs -> IBM Content Manager for Multiplatforms V8.2 -> First Steps**

__ 2. Click on **Load Sample Data**.

An input panel appears. The following example shows the values you should enter if you selected the default values during the installation program:

```
Library server database name:      ICMNLSDB
Resource manager database name:    RMDB
User Id:                           icmadmin
Password:                          password
```

Wait several minutes for the sample data to be loaded. An hour glass pops up indicating the progress. When you see the hour glass disappear, the sample data has been created. Check the following file to see if the first steps program succeeded:

```
%ICMROOT%\BIN\FirstSteps\cm\icmcrsample.log
```

It should reflect the successful loading of the sample database and end saying:

```
Datastore disconnected
```

__ 3. Click on **Work with Sample Data**. This starts the System administration client. (Alternatively, go to **Start -> Programs -> IBM Content Manager for Multiplatforms V8.2 -> System Administration**).

__ 4. Continue with "Validating the first steps" on page 159.

Running First Steps for a multiple machine Content Manager system

Start the first steps procedure here if you installed the Content Manager components on more than one machine, even if the components are on different operating systems:

__ 1. Ensure administration client (installed on this Windows machine) is configured to connect to a remote administration database.

__ 2. Make sure that the library server database is already installed (either on this local machine or on a **remote** database machine.

__ 3. Make sure that the resource manager database is already installed (either on this local machine or on a **remote** database machine.

__ 4. Catalog the remote database(s) on the local client.

To catalog the database, run the DB2 Client Configuration Assistant and follow the system prompts. (For example, to start the Configuration Assistant on DB2 Version 8, click **Start** ⟶ **Programs** ⟶ **IBM DB2** ⟶ **Set-up Tools** ⟶ **Configuration Assistant**.)

__ 5. Configure the (ICMNLSDB) remote database for use with the Content Manager Administration Client by clicking: **Start -> Programs -> IBM Content Manager for MultiPlatforms V8.2 -> Server Configuration Utility**

Enter the configuration information as follows:

Server type:
Content Manager

Server name:
ICMNLSDB

Schema name:
ICMADMIN

Host name:
<Host name>

Operating system:
<Operating system>

Port number:
50000 (Default DB2 port number)

Security options:
Server authentication (Default)

User ID:
icmadmin

Password:
<password>

__ 6. Click on **Load Sample Data**. The following shows the values you should enter if you selected the default values during the install:

```
Database name:          ICMNLSDB
Database schema:        ICMADMIN
User Id:                icmadmin
Password:               password
```

Wait several minutes for the sample data to be loaded. An hour glass will pop-up indicating progress. Once you see the hour glass disappear the sample data has been created.

__ 7. 4) Click on **Work with Sample Data**. This starts the System administration client. Continue to the next section: "Validating the first steps".

Validating the first steps

__ 1. The System Administration Client logon panel should appear. Make sure that **Content Manager** and the correct database are selected from the drop-down lists. Log in with the DB2 administration ID you specified for the Library Server database during the Content Manager installation, for example: icmadmin.

Successful logon means that your communication between the Library Server and the System Administration Client is working and also indicates that the Library Server database has been created.

Verify the data was loaded by looking for the sample item type definitions beginning with the prefix XYZ

__ 2. You can also check to see if content was loaded into the Resource manager by looking for the RM staging and destaging directories. If you selected the default locations during CM install, you can look for files in `C:\LBOSDATA\00001\01` after running CM First Steps. The staging directory is `C:\STAGING`.

__ 3. If you get an error with First Steps, go through the previous verification steps under Chapter 11, "Verifying a successful installation of Content Manager on Windows", on page 153.

The following sections cover Library server validation:

"Verify library server database" on page 153

"Verify library server access modules generated" on page 154

The final three sections cover Resource manager validation:

"Verify resource manager deployment" on page 155

"Verify resource manager Web application in a Web browser" on page 156

"Verify resource manager database" on page 156

__ 4. If the following CM First Steps 'Load sample data' problem error occurs

```
[IBM][CLI Driver] CLI0123E  SQL data type out of range.
                                                 SQLSTATE=HY004
```

Rerun `usejdbc2.bat` to ensure the JDBC upgrade from version 1 to 2:

__ Step a. Run First Steps and click **Remove Sample Data** option

__ Step b. Stop DB2 JDBC Applet Server service

__ Step c. Run `usejdbc2.bat` located in SQLLIB\java12 directory (e.g. `c:\program files\sqllib\java12`)

__ Step d. Restart DB2 JDBC Applet Server service

__ Step e. Run First Steps and click 'Load Sample Data' option

__ Step f. Check the icmcrsample.log (e.g. c:\program files\ibm\cm81\bin\firststeps\cm) for the following lines:

```
Connecting to datastore...
Datastore connected.

Creating sample attributes...

Attribute XYZ_ClaimNumber was created successfully.
Attribute XYZ_DriversLic was created successfully.
Attribute XYZ_LicPlate was created successfully.
Attribute XYZ_PolicyNum was created successfully.
Attribute XYZ_ReportNum was created successfully.
Attribute XYZ_State was created successfully.
Attribute XYZ_VIN was created successfully.
Attribute XYZ_ZIPCode was created successfully.
Attribute XYZ_AdjustFName was created successfully.
Attribute XYZ_AdjustLName was created successfully.
Attribute XYZ_City was created successfully.
Attribute XYZ_ClaimFName was created successfully.
Attribute XYZ_ClaimLName was created successfully.
Attribute XYZ_InsrdFName was created successfully.
Attribute XYZ_InsrdLName was created successfully.
Attribute XYZ_Street was created successfully.
Attribute XYZ_Type was created successfully.
Attribute XYZ_AdjustDate was created successfully.
Attribute XYZ_IncDate was created successfully.

Creating sample item types...

Item type XYZ_ClaimForm was created successfully.
Item type XYZ_AdjReport was created successfully.
Item type XYZ_PolReport was created successfully.
Item type XYZ_InsPolicy was created successfully.
Item type XYZ_AutoPhoto was created successfully.

Creating sample items...

A DDO of item type XYZ_ClaimForm was created successfully.
A DDO of item type XYZ_ClaimForm was created successfully.
A DDO of item type XYZ_ClaimForm was created successfully.
A DDO of item type XYZ_AdjReport was created successfully.
A DDO of item type XYZ_AdjReport was created successfully.
A DDO of item type XYZ_AdjReport was created successfully.
A DDO of item type XYZ_PolReport was created successfully.
A DDO of item type XYZ_PolReport was created successfully.
A DDO of item type XYZ_PolReport was created successfully.
A DDO of item type XYZ_InsPolicy was created successfully.
A DDO of item type XYZ_InsPolicy was created successfully.
A DDO of item type XYZ_InsPolicy was created successfully.
A DDO of item type XYZ_AutoPhoto was created successfully.
A DDO of item type XYZ_AutoPhoto was created successfully.
A DDO of item type XYZ_AutoPhoto was created successfully.

Disconnecting from datastore...
Datastore disconnected.
```

Verifying that DB2 Universal Database Relational Connect is set up correctly for Oracle

After the software is installed, a user with SYSADM authority should check the setup and create the federated database. The DB2 instance owner then configures the server to access the Oracle data sources.

Checking the federated server setup

After the federated server is setup, you can avoid potential problems by checking the following key setting:

- Ensure that the FEDERATED parameter is set to YES.

Checking for the wrapper library files

The link-edit scripts create the wrapper libraries in specific directories, depending on the operating system. The following tables list the directory path for the library file names by data source. If the wrapper library file appears in the directory, the link-edit was successful.

Oracle:

The directory paths and wrapper library file names for Oracle.

The wrapper library names for Oracle are:

Table 70. Oracle wrapper library names

Operating system on your federated server	Wrapper library names for SQLNET	Wrapper library names for NET8
AIX	libdb2sqlnet.a	libdb2net8.a
Solaris	libdb2sqlnet.so	libdb2net8.so
Windows NT and Windows 2000	db2sqlnet.dll	db2net8.dll

Checking the link-edit error message files

If the link-edit fails, there will be errors listed in the error message file in the library directory. There may be an error message file in the library directory, even if the link-edit is successful. You need to open the error message file to determine if the link-edit failed. The link-edit error message file names are listed in the following table.

Table 71. Link-edit error message file names by data source

Data source	Error message file names
Oracle	djxlinkOracle.out

Manually linking DB2 to the data source client libraries

The link script creates the wrapper libraries on the federated server for the data source you are setting up. There are several reasons why the link might fail when you setup the federated server:

- If the client software is not installed before the link-edit is attempted, then the link-edit will fail. For example, if you do not install the Informix client software before you install the DB2 server software, the link-edit will fail. Likewise, if you do not install the Sybase Open Client software before you install DB2 Relational Connect, the link-edit will fail. In these situations, you will have to perform the link manually.
- Check to make sure the version of the data source client is supported. The latest information is on the product Web sites. Check the DB2 Relational Connect Web sitewww.ibm.com/software/data/db2/relconnect/. If the

version of the data source client you have installed is not supported, the link-edit will fail. You will have to install a client version that is supported and then perform the link manually.

You need root authorization to run the link scripts. The quickest way to link DB2 to the data source client libraries is:

__ 1. Install and configure the client software on the DB2 federated server (if necessary).

__ 2. Use the product CDs and run the DB2 Relational Connect installation again.

If you manually run a link script, you must issue the **db2iupdt** command on each DB2 instance to enable federated access to the data sources.

Note: There is another script, the `djxlink` script, that attempts to create a wrapper library for every data source that DB2 for UNIX and Windows supports. If you only have the client software for some of the data sources installed, you will receive an error message for each of the missing data sources when you issue the `djxlink` script.

Once the link is performed, check the permissions on the wrapper libraries after they are created. Make sure that the libraries can be read and executed by the DB2 instance owners.

Creating the federated database

After you setup the federated server, the DB2 instance owner creates a DB2 database on the federated server instance that will act as the federated database.

You can create the database two ways:

- Through the DB2 Control Center
- Through the DB2 Command Center or DB2 command line processor (CLP).

The advantage of using the DB2 Control Center is that you do not have to key in each statement and command. It is the easiest way to quickly create a database.

The steps in this section assume that you are using the DB2 Command Center or the command line processor (CLP) to create the database.

Prerequisites:

A federated server that is properly setup to access your data sources. This includes the installation and configuration of any required software, such as:

- Client software

- DB2 Relational Connect

Restrictions:

You need SYSADM or SYSCTRL authority to create a DB2 database.

Procedure:

Create a DB2 database on the federated server instance that will act as the federated database. For example:

```
CREATE DATABASE federated
```

This command:

- Initializes a new database.
- Creates the three initial table spaces.
- Created the system tables.
- Allocates the recovery log.

In a multi-node environment, this command affects all nodes that are listed in the db2nodes.cfg file. The node from which this command is issued, becomes the catalog node for the new database.

Adding Oracle data sources to a federated server

Configuring the federated server to access Oracle data sources involves supplying the server with information about the Oracle data sources and objects you want to access. You can configure access to Oracle data sources two ways:

- Through the DB2 Control Center
- Through the DB2 Command Center or command line processor (CLP)

The advantage of using the DB2 Control Center is that you do not have to key in each statement and command. It is the easiest way to quickly configure access to Oracle data sources. There are a few configuration tasks that can not be accomplished through the DB2 Control Center:

- Setting up and testing the Oracle client configuration file.
- Testing the connection to the Oracle server to validate the server definition and user mappings.
- Adding or dropping column options.

The steps in this section assume that you are using the DB2 Command Center or the command line processor (CLP) to configure access to Oracle data sources.

Prerequisites:

- A federated server and database that are setup to access Oracle data sources.
- The Oracle client software installed and configured on the federated server.
- The proper variables setup. This includes: system environment variables, db2dj.ini variables (UNIX only), and DB2 Profile Registry (db2set) variables.

The steps to accomplish these tasks are discussed in "Before you begin to install IBM DB2 Universal Database" on page 88.

Procedure:

To add an Oracle data source to a federated server:

1. Set up and test the Oracle client configuration file.
2. Create the wrapper.
3. Create the server definition and set the server options.
4. Create the user mappings.
5. Test the connection to the Oracle server.
6. Create nicknames for Oracle tables and views.

These steps are explained in detail in this section. Operating system-specific differences are noted where they occur.

Step 1: Set up and test a client configuration file: The client configuration file is used to connect to Oracle databases, using the client libraries that are installed on the federated server. This file specifies the location of each Oracle database server and type of connection (protocol) for the database server. The default name for the Oracle client configuration file is `tnsnames.ora`.

To set up the client configuration file, use the utility that comes with the Oracle client software. See the installation documentation from Oracle for more information about using this utility. Within the `tnsnames.ora` file, the SID is the name of the Oracle instance, and the HOST is the host name where the Oracle server is located.

The Windows directory in which the `tnsnames.ora` file is created is `%ORACLE_HOME%\NETWORK\ADMIN`

Test the connection to ensure that the client software is able to connect to the Oracle server. Use the Oracle **sqlplus** tool to test the connection.

Setting a different location for the tnsnames.ora file: If you decide to place the `tnsnames.ora` file in a path other than the default search path, you must set the TNS_ADMIN environment variable to specify the file location. To set this environment variable:

__ 1. Edit the db2dj.ini file located in the sqllib/cfg directory, and set the TNS_ADMIN environment variable:

```
TNS_ADMIN=x:\path\tnsnames.ora
```

__ 2. To ensure that the environment variable is set in the program, recycle the DB2 instance. Issue the following commands to recycle the DB2 instance:

```
db2stop
db2start
```

Step 2: Create the wrapper: To specify the wrapper that will be used to access Oracle data sources, use the CREATE WRAPPER statement. DB2 Relational Connect includes two wrappers for Oracle. To determine which wrapper to use, consult the following:

For Oracle Version 7
Use the SQLNET wrapper.

For Oracle Version 8
Use the NET8 wrapper (recommended) or the SQLNET wrapper.

For Oracle Version 9
Use the NET8 wrapper (recommended) or the SQLNET wrapper.

Note: The SQLNET wrapper uses OCI 7 (Oracle Call Interface) API calls. The NET8 wrapper uses OCI 8 API calls. If the Oracle 8 or Oracle 9 client is installed, you will experience better performance and functionality by using the NET8 wrapper. Additionally, the NET8 wrapper has LOB support. Because the OCI 7 does not support LOB data types, the SQLNET wrapper does not support Oracle LOB data types.

- The SQLNET wrapper maps Oracle LONG data types to DB2 for UNIX and Windows LOB data types.
- The NET8 wrapper does not support Oracle LONG data types. It does map Oracle LOB data types to DB2 for UNIX and Windows LOB data types.

The following example shows the CREATE WRAPPER statement for the NET8 wrapper:

```
CREATE WRAPPER NET8
```

Recommendation: Use the default wrapper names (SQLNET or NET8). When you create the wrapper using one of the default names, the federated server automatically picks up the default library name associated with the wrapper. If the wrapper name conflicts with an existing wrapper name in the federated database, you can substitute the default wrapper name with a name you choose. If you use a name that is different than one of the default names, you must include the LIBRARY parameter in the CREATE WRAPPER statement.

Suppose that you have a federated server running on AIX and you decide to use a wrapper name that is not one of the default names. Examples of the CREATE WRAPPER statements for SQLNET and NET8 are:

```
CREATE WRAPPER mywrapper LIBRARY 'libdb2sqlnet.a'
```

```
CREATE WRAPPER mywrapper LIBRARY 'libdb2net8.a'
```

The wrapper library names for Oracle are:

For SQLNET
The wrapper library name is: `db2sqlnet.dll`

For NET8
The wrapper library name is: `db2net8.dll`

Step 3: Create the server definition: In the federated database, you must define each Oracle server that you want to access. You create a server definition using the CREATE SERVER statement. For example:

```
CREATE SERVER oraserver TYPE oracle VERSION 7.2 WRAPPER net8
OPTIONS (NODE 'paris_node')
```

oraserver
A name that you assign to the Oracle database server. This name must be unique. Duplicate server names are not allowed.

TYPE *oracle*
Specifies the type of data source server to which you are configuring access. The type parameter for the `SQLNET` and `NET8` wrappers must be *oracle*.

VERSION *7.2*
The version of Oracle database server that you want to access. The supported Oracle versions are 7.x, 8.x, and 9.x.

WRAPPER *net8*
The name you specified in the CREATE WRAPPER statement.

NODE *'paris_node'*
The name of the node where the Oracle database server resides. Obtain the node name from the `tnsnames.ora` file.

Although the node name is specified as an option in the CREATE SERVER statement, it is required for Oracle data sources.

Locating the node name: You must define the node name in the Oracle `tnsnames.ora` file (see step 1). Although the *node_name* is specified as an option in the CREATE SERVER statement, it is required for Oracle data sources. This is an example of a `tnsnames.ora` file:

```
ORA9I.SEEL =
  (DESCRIPTION =
  (ADDRESS_LIST =
     (ADDRESS = (PROTOCOL = TCP)(HOST = somehost)(PORT = 1521)))
     (CONNECT_DATA =
     (SERVICE_NAME = ora9i.seel)))
```

The node value to use in the CREATE SERVER statement would be `ora9i.seel`.

Optional: Set additional server options: When you create the server definition, you can specify additional server options in the CREATE SERVER statement. There are general server options and data source-specific server options.

DB2 assumes that all of the Oracle VARCHAR columns contain trailing blanks. If you are certain that all VARCHAR columns in the Oracle database do not contain trailing blanks, you can set a server option to specify that the data source uses a non-blank padded VARCHAR comparison semantic. An example of the CREATE SERVER statement with this server options is:

```
CREATE SERVER oraserver TYPE oracle VERSION 7.2 WRAPPER net8
OPTIONS (NODE 'paris_node', VARCHAR_NO_TRAILING_BLANKS 'Y')
```

Use the VARCHAR_NO_TRAILING_BLANKS server option when all the columns do not contain trailing blanks. If only ssome of the VARCHAR columns do not contain trailing blanks, you can set an option on those specific columns with the CREATE NICKNAME or ALTER NICKNAME statements.

After the server definition is created, use the ALTER SERVER statement to add or drop server options.

Step 4: Create the user mappings: When you attempt to access an Oracle server, the federated server must first establish a connection to the data source. The federated server does this by using a valid user ID and password to that data source. You must define an association between the federated server user ID and password and the data source user ID and password. This association must be created for each user ID that will be using the federated system to send distributed requests. This association is called a *user mapping*.

Use the CREATE USER MAPPING statement to map the local user ID to the Oracle server user ID and password; for example:

```
CREATE USER MAPPING FOR robert SERVER oraserver
OPTIONS (REMOTE_AUTHID 'rob', REMOTE_PASSWORD 'then4now')
```

robert The local user ID that you are mapping to a user ID defined at an Oracle server.

SERVER *oraserver*
The name of the Oracle server that you defined in the CREATE SERVER statement.

REMOTE_AUTHID *'rob'*
Tthe user ID at the Oracle database server to which you are mapping *robert*. This value is case sensitive unless you set the FOLD_ID server option to 'U' or 'L' in the CREATE SERVER statement.

REMOTE_PASSWORD *'then4now'*
The password associated with *'rob'*. This value is case sensitive unless you set the FOLD_PW server option to 'U' or 'L' in the CREATE SERVER statement.

You can use the DB2 special register **USER** to map the authorization ID of the person issuing the CREATE USER MAPPING statement to the data source authorization ID specified in the **REMOTE_AUTHID** user option. The following is an example of the CREATE USER MAPPING statement which includes the **USER** special register:

```
CREATE USER MAPPING FOR USER SERVER oraserver
OPTIONS (REMOTE_AUTHID 'rob', REMOTE_PASSWORD 'then4now')
```

Restriction: The user ID at the Oracle data source must have been created using the Oracle create user command with the 'identified by' clause, instead of the 'identified externally' clause.

Step 5: Test the connection to the Oracle server: Test the connection to the Oracle server to ensure that you can establish a connection, using the server definition and user mappings you defined. Open a pass-through session and issue a SELECT statement against the Oracle system tables. For example:

```
SET PASSTHRU server_name
SELECT count(*) FROM sys.all_tables
SET PASSTHRU RESET
```

If the SELECT returns a count, then your server definition and user mapping are set up properly. If the SELECT returns an error, you might have to:

- Check the Oracle server to make sure that it is configured for incoming connections.
- Check your user mapping to make sure that the settings for the REMOTE_AUTHID and REMOTE_PASSWORD options are valid for connections to the Oracle server.
- Check the Oracle client software on the DB2 federated server to make sure that it is installed and configured correctly to connect to the Oracle server.

- Check your DB2 federated variables to make sure that they are correct for working with the Oracle server. This includes checking the system environment variables, db2dj.ini variables, and the DB2 Profile Registry (db2set) variable.
- Check your server definition and possibly drop it and create it again.
- Check your user mapping and possibly alter it or create another if necessary.

Step 6: Create the nicknames for tables and views: The federated database relies on catalog statistics for nicknamed objects to optimize query processing. These statistics are gathered when you create a nickname for a data source object using the CREATE NICKNAME statement. The federated database verifies the presence of the object at the data source, and then attempts to gather existing data source statistical data. Information useful to the optimizer is read from the data source catalogs and put into the global catalog on the federated server. Because some or all of the data source catalog information might be used by the optimizer, update statistics (using the data source command equivalent to RUNSTATS) at the data source before you create a nickname.

For each Oracle server you defined, assign a nickname to each table or view you want to access on those servers. You will use these nicknames, instead of the names of the data source objects, when you query the Oracle servers. Nicknames can be up to 128 characters in length.

The federated server will fold the Oracle server, schema, and table names to uppercase unless you enclose them in double quotation marks ("). The following example shows a CREATE NICKNAME statement:

```
CREATE NICKNAME PARISINV FOR oraserver."france"."inventory"
```

:

PARISINV

A unique nickname used to identify the Oracle table or view.

Note: the nickname is a two-part name—the schema and the nickname. If you omit the schema when creating the nickname, the schema of the nickname will be the authorization ID of the user creating the nickname.

oraserver."france"."inventory"

A three-part identifier for the remote object:

- *oraserver* is the name you assigned to the Oracle database server in the CREATE SERVER statement.
- *france* is the name of the remote schema to which the table or view belongs.

- *inventory* is the name of the remote table or view that you want to access.

Repeat this step for each Oracle table or view for which you want create nicknames. When you create the nickname, DB2 will use the connection to query the data source catalog. This query tests your connection to the data source using the nickname. If the connection does not work, you will receive an error message.

Tuning and troubleshooting the configuration to Oracle data sources

After you have set up the configuration to Oracle data sources, you may want to modify the configuration to improve performance.

Connectivity problems: For each HOST in the DESCRIPTION section of the `tnsnames.ora` file, you might need to update the `hosts` file. Whether you update this file depends on how TCP/IP is configured on your network. Part of the network must translate the remote host name specified in the DESCRIPTION section in the `tnsnames.ora` file to an address. If your network has a named server that recognizes the host name, you do not need to update the TCP/IP `hosts` file. Otherwise, you need an entry for the remote host. See your network administrator to determine how your network is configured. If you need to update the `hosts` file, the file location depends on the federated server operating system:

On Windows federated servers

Update the `x:\winnt\system32\drivers\etc\hosts` file.

Chapter 12. Installing Enterprise Information Portal components on Windows

This section explains how to install EIP components on Windows servers.

Before you install the administration database

Read this section before you install any administration database, including the information mining database, and the Content Manager Version 8 connector, or if you plan to add EIP tables to Content Manager Version 8 databases.

Sharing a Content Manager Version 8 database

Because EIP Version 8 and Content Manager Version 8 share common code, you can share a Content Manager Version 8 library server database.

Restriction: If you plan to share the library server database, you must be sure that the database was Unicode-enabled during installation and that the code page is 1208. There are two ways to check whether the database meets the requirements.

Use a DB2 command window (Start→Programs-→IBM DB2→Command Window)

1. At the prompt, type `db2 get db cfg for <Content Manager Version 8 database>`
2. Check that the `Database code page` setting is `1208`

Use the DB2 Control Center (Start→Programs-→IBM DB2→Control Center)

1. Highlight the Content Manager Version 8 database.
2. Right-click Configure. The Environment tab appears.
3. Check that the `Database code page` value is `1208`.

If you plan to share a Content Manager Version 8 library server database, you must know the user IDs that were defined when that specific Content Manager Version 8 database was installed. This is required because the EIP installation program uses the user ID to access the Content Manager Version 8 database, add the EIP tables and save the modified database.

The Content Manager Version 8 database must be on a local drive of the server where you are installing EIP. You cannot add EIP tables to a Content Manager Version 8 database that is accessed through a networked drive.

You must start DB2 on the server that contains the Content Manager Version 8 Library Server database you are sharing with EIP.

Because you are you are modifying an existing DB2 database, you must log on to the server with a user ID and password that allows you to administer DB2 databases.

You must define exactly the same Server name, Schema name, user ID and password that was used when the Content Manager Version 8 database was created.

Are you installing an administration database *and* the Content Manager Version 8 connector?

If you install the Content Manager Version 8 connector, you must know the user IDs and passwords defined when the Content Manager Version 8 database that you want to connect to was installed. You must perform the following steps:

1. On the window labeled Identify Administration Database, you must enter one administration user ID and one DB2 Connect user ID. The administrator and the Connect user ID must be locally defined. **Requirement:** If you are sharing a Content Manager Version 8 library server, you must type the same administrator user ID and the Connect user IDs defined when the Content Manager database you are sharing was created.
2. On the window labeled Configure Federated Server Connection, you must type the password associated with the DB2 Connect user ID.
3. On the Configure Content Manager Version 8 connector window, type the DB2 Connect user ID and password that was defined when the Content Manager Version 8 library server database was installed.

Are you installing an administration database but *not* the Content Manager Version 8 connector?

See steps 1 and 2 in the previous section.

Are you sharing a Content Manager Version 8 database?

You must perform the following steps:

1. If you are sharing a Content Manager Version 8 library server, you must type the same administrator user ID and the Connect user ID defined when the Content Manager database you are sharing was created.
2. On the window labeled Configure Federated Server Connection, type the DB2 Connect user ID and password that was defined when the Content Manager Version 8 Library Server database was installed.

3. On the Configure Content Manager Version 8 connector window, type the DB2 Connect user ID and password that was defined when the Content Manager Version 8 library server database was installed.

Restriction! The Database connection user IDs (and all other values) you define in steps 1, 2 and 3 of this section must be the same in each window.

Removing previous versions of EIP

The uninstall program removes the EIP components from previous versions. The databases are not removed because they are stored in DB2. The EIP uninstall program detects changes to `*.INI` and `*.BAT` files and prompts you to decide if you want to make backup copies of these files.

1. Click **Start⟶Programs-⟶IBM Enterprise Information Portal for Multiplatforms⟶Uninstall**.
2. Select the language from the **Choose Setup Language** window, click **OK**, then click **Yes** to start the component removal process.
3. To remove modified `*.INI` or `*.BAT` files from `cmbroot`, click **Yes**. If you click **No**, the program prompts you to decide if you want to make backup copies of the `*.BAT` and `*.INI` file. If you click Yes, the program stores the backup files in `cmbroot`.
4. Click **Yes** or **No** and click **Finish**.
5. After you restart the workstation, copy backup `*.INI` or `*.BAT` files to a temporary directory.
6. Delete the `\CMBROOT` directory.

EIP Windows installation quick start

1. Insert the EIP Windows installation CD-ROM in the CD-ROM drive. If the program begins automatically, select the appropriate language and click **Next**. If the installation does not start automatically, navigate to the CD-ROM drive, select the appropriate language directory and double-click `setup.exe`.
2. Click **Accept** to accept the License Agreement. The Select Machine Type Window appears.
3. Click a Machine Type and click **Next**.
   - Client
   - Server
   - Development Workstation
4. Click **Next** to accept the default path and directory name for the EIP product and for the configuration files, or change the path and name information as required.
5. Click the appropriate components and subcomponents and click **Next**.

6. Depending on the components you install, and on your system plan, the program displays various installation windows and prompts you to type configuration information.
7. Click **Finish** and restart the server.

EIP installation windows

Table 72 lists the common EIP installation windows you always see, in the general sequence you see them, no matter which components you select. When you install some components, such as the Information Center or IBM Web Crawler, you see only the common installation windows.

When you install other components, you will see specific windows. Table 73 on page 177 lists the specific windows in alphabetical order. The installation sequence and the windows you see varies, depending on the components you install. For example, you will only see the VisualInfo for AS/400 Network Table Generation window if you select the CM for AS/400 connector.

Table 72. Common EIP installation windows

Common window	**Details**
License Agreement	See "Software License Agreement" on page 179.
Select Machine Type	See "Select Machine Type" on page 179.
Specify Destination	See "Specify Destination" on page 179.
Component Selection	See "Component Selection" on page 180.
Specify RMI Host Name and Port Number	See "Specify RMI Host Name and Port Number" on page 180.
System Configuration	See "System Configuration" on page 180.
Start Copying Files	See "Start Copying Files" on page 183.
Product Registration	See "Product Registration" on page 183.
Installation Complete	See "Installation Complete" on page 183

Table 73. Specific EIP installation windows

Specific window	Description	Details
Catalog remote database	The values you define in this panel enable communications between the administration client and a remote EIP database.	For information on how to collect the information required to fill out this window, see "Connecting the administration client to a remote administration database" on page 447.
Configure components for LDAP	You use this window to enable the administration database and/or the administration client to use LDAP information.	See "Configure Components for LDAP" on page 183.
Configure Content Manager V8 Server Connection	Only used when you install the Content Manager Version 8 connector.	See "Configure Content Manager V8 Server Connection" on page 184.
Configure federated server connection	Only used when you install: • the administration client and/or • any connector	See "Configure Federated Server Connection" on page 184.
Configure LDAP Server	Only used when you install: • the common configurations on an LDAP server and • the federated connector and • the Content Manager Version 8 connector and • the administration or Information Mining database	See "Configure LDAP Server" on page 183.
Define LDAP Server	Only used when you install: • the common configurations on an LDAP server and • the federated connector and • the Content Manager Version 8 connector and • the administration or Information Mining database	See "Define LDAP Server" on page 185.

Table 73. Specific EIP installation windows (continued)

Specific window	Description	Details
Destination Path for Content Manager V7 connector C-APIs	Only used when you install the Content Manager Version 7 connector.	See "Destination Path for Content Manager V7 Connector C-APIs" on page 186.
Existing database	Only used when you install: • The administration database and/or Information Mining feature and • You share the EIP tables in a Content Manager Version 8 Library Server database.	See "Existing Database" on page 186.
Identify Administration Database	Only used when you install an administration or Information Mining database.	See "Identify Administration Database" on page 186.
Image Search Server/Client Configuration	Only used when you select the Image Search feature.	See "Image Search Server/Client Configuration" on page 188
Install OnDemand?	Only used when you install the OnDemand viewer.	See "Install OnDemand?" on page 188.
Network Table Generation	Only used when you install the Content Manager Version 7 connector. This window gives you options to generate the Content Manager Version 7 network table.	See "Network Table Generation (for Content Manager version 7 connector)" on page 188
Network Table Generation	Only used when you install the Content Manager Version 7 connector. The values you type are copied to the Content Manager Version 7 network table (`FRNROOT/FRNOLINT.TBL`).	See "Network Table Generation (for Content Manager version 7 connector)" on page 189
Select administration database options	Only used when you install a new database or replace an existing database.	See "Select Administration Database Options" on page 190.

Table 73. Specific EIP installation windows (continued)

Specific window	Description	Details
Select Version of VisualInfo for AS/400	Only used when you install the VisualInfo for AS/400 connector.	See “Select Version of VisualInfo for AS/400” on page 190
Server configuration utility	Used to define port number, database name and other information about remote databases.	
Text Search Server/Client Configuration	Only used when you select the Text Search feature.	See “Text Search Server/Client Configuration” on page 190.
Upgrade OnDemand?	Only used when you install the OnDemand viewer *and* you have an existing OnDemand client on the server.	“Upgrade OnDemand?” on page 191
VisualInfo for AS/400 Network Table Generation	Only used when you install the VisualInfo for AS/400 connector. You type the values that are part of the VisualInfo for AS/400 network table.	

Common installation windows

This section describes the installation windows that you will see when you install any EIP component.

Software License Agreement

Click **Accept** to accept the license agreement. Click **Decline** to end the installation.

Select Machine Type

Click Client, Server or Development Workstation and click **Next.**

Server Configuration Utility

| On this window, you enter the database name, server port number and other
| information required to connect to a remote database.

Specify Destination

On this window, you can change the default installation paths and directory names for the for `CMBROOT` and for `CMgmt`. `CMBROOT` contains the EIP program, and `CMgmt` contains the common configuration files. The information you define in this window is stored in the Windows environment system variables.

Type new information in one or both fields, or click Next to accept the default path and file names.

Component Selection

On this window, you select the components to install. You can install all components at the same time, or select individual components.

Specify RMI Host Name and Port Number

On this window, you define RMI host name and port number for an RMI server and you can also define an RMI host name and port number for a workflow or Information Mining RMI server.

If your system plan includes a master RMI server, type the host name of the master server and the master server port number in the fields in the top half of this window. The default host name is the local server name, and the default port number is 1919. The RMI information is copied to `x:\<CMCOMMON>\cmbclient.ini`. **Tip:** Ask the server administrator if you are required to enter a fully-qualified master RMI server host name.

If your system plan includes a separate RMI server for workflow or Information Mining, type the host name and port number for the workflow or Information Mining RMI server in the fields in the bottom half of this window. This RMI information is copied to `x:\<CMBROOT>\cmbsvclient.ini`

Tip: If your system plans include RMI, you must install and configure the connectors on the RMI server in a separate step before the clients can use the RMI server.

System Configuration

EIP Version 8 offers a new option that allows EIP components to access remote system configuration files across a network or Web server.

For example, you can install the configuration files on a network server in Chicago, install administration databases in the Seattle and San Francisco offices, and an administration client in New York. All users would access their required configuration files in Chicago through a network drive.

The selections you make on the System Configuration window define the location of the system configuration files. The system configuration files are in a directory named `CMgmt`. The files in `CMgmt` contain information used by the administration client, connectors and other EIP components. For example, the administration client needs the information stored in the configuration file named `cmbds.ini` to connect to the administration database. Another configuration file, `cmbicmsrvs.ini`, contains data required to catalog, connect to and search a Content Manager Version 8 server. The window also gives you the option to point remote components to a data source file stored on an LDAP server.

Restrictions

- The configuration files do not have to be installed on the network or Web server when you define the path, but the files must be installed before any user can work with EIP. To install the configuration files on a network or Web server, you can use the EIP installation CD-ROM, or, if you have already installed configuration files on another server, you can copy the `CMgmt` directory to the network or Web server.
- Before remote EIP components can access and use configuration files on a network server, you must configure the following properties:
  - Set up sharing on the configuration file directories and subdirectories. The configuration files that can be accessed across a network are installed in `CMgmt`, and the subdirectories are `admin`, `doc`.
  - Define user IDs and passwords for the remote users on the server where you installed the shared configuration files.
  - Be sure the user IDs and passwords have read/write privileges. Read/write access is required because the clients and other components update shared configuration files, including log files.
- If you install the configuration files on a Web server, see the Web administrator for information on configuring sharing and read/write parameters for remote EIP users.
- If you are installing the Information Center, you must select Local to install the system configuration files. The Information Center files are installed in `CMgmt/infoctr`. Users cannot access the Information Center through a network or Web server.
- If you plan to point remote users to data source configuration information stored on an LDAP server, you must use a utility specific to your LDAP product to install only the data source configuration file. See your LDAP administrator for more information. The data source file is named `cmbds.ini`.
- The option to point remote users to a data source file stored on an LDAP server is only selectable if:
  - You are installing the Content Manager Version 8 connector and
  - You are installing the federated connector by itself and/or
  - You are installing the administration database, the Information Mining database, or the administration client, because the federated connector is always installed with those components.

This section describes the fields on the System Configuration window.

Local Click **Local** to install the configuration files on the local server. The configuration files are installed in `<CMgmt>`, using the path and directory name you defined in the Specify Destination window.

Remote

Click **Remote** and type the path where you installed, or plan to install, the configuration files on a network server.

Tip: If you have already installed, or plan to install, Content Manager Version 8, EIP can share the Content Manager configuration files across a network. Click **Remote** and type in the path where you installed or plan to install the Content Manager configuration files.

Web Server

Type the URL of the Web server where you installed, or plan to install, the configuration files. The configuration files do not have to be installed on the Web server when you type the URL, but they must be installed before any user can work with EIP. Contact the Web administrator to learn more about how remote EIP users can connect to and update configuration files on a Web server.

Tip: If you have already installed, or plan to install, Content Manager Version 8, EIP can share the Content Manager configuration files. Type the URL where you installed or plan to install the Content Manager Version 8 configuration files.

Use datasource configuration information stored on an LDAP server

Click this box to begin the process of defining and configuring LDAP server information so you can later install the `cmbds.ini` configuration file. You do not have to install an LDAP server to select this option. But you must know specific information about the LDAP server. If you click this box and press **Next**, the installation program displays the **Define LDAP Server** and **Configure LDAP Server** windows. The information you define on those two windows is stored in the `cmbcmenv.properties` file for later use by the administration client and other EIP components. **Tip**: if the installation program detects an existing `cmbcmenv.properties` file, you cannot modify any of the fields in Define LDAP Server and Configure LDAP Server windows

You install the configuration files on the LDAP server in a separate step using an LDAP utility after you install EIP. For more information, see the LDAP server documentation.

You see **Define LDAP Server** and **Configure LDAP Server** only if you:

- Click LDAP server on the System Configuration window and
- Install the Content Manager Version 8 connector and
- Install the federated connector either by itself of as part of an administration of Information Mining database

Start Copying Files

This window shows all components that you selected for installation. Click **Next** to begin installation, or click **Back** to change your component selections. When you click **Next**, EIP displays multiple messages describing the component installation status.

Product Registration

Type the information required to register EIP Version 8.2. Click **Next** to send the registration to IBM, or click **Exit** to send the registration information at a later time.

Installation Complete

Click Yes, I want to restart my computer now or No, I will restart my computer later and click **Finish**.

Specific installation windows

This section describes the windows that are specific to some components, such as the administration database. Depending on system design, you might see some or all of these windows. **Tip:** The windows are described in alphabetical order, because the sequence in which you see the windows depends on the components you are installing.

Configure Components for LDAP

In this window, you can choose to enable the system administration database and the client to use information imported from an LDAP server. Click System administration database to enable the database for LDAP, and click System administration client to enable the client to import users from an LDAP server. You can select one or both options. If your system plan does not include LDAP, click **Next**.

Configure LDAP Server

On this window, you define the LDAP Server Base distinguished name and User authentication attributes. EIP stores the information from this window in `cmbcmenv.properties`. **Tip:** You are not required to install, configure or start any LDAP servers before you define the information required on this window.

Base distinguished name
Select IBM Secureway or Microsoft Active Directory. Type the base distinguished name

Hostname
Type the LDAP server host name.

Port
Type the LDAP server port number.

LDAP administration ID
Type the LDAP administration user ID.

Password
Type the LDAP administration password.

Configure Content Manager V8 Server Connection

On this window, you define the information required to connect to the Content Manager Version 8 server. You only see this window if you install the Content Manager Version 8 connector. When the administrator defines and connects to a Content Manager Version 8 server, EIP uses the values you define in this window to connect to the server. By default, EIP copies the information from this window to `cmbicmsrvs.ini` and `cmbicmenv.ini`.

Database name
Type the Content Manager Version 8 database name. If you have cataloged the database, type the alias name in this field.

Schema name
Type the schema name that was assigned to the Content Manager Version 8 database when the database was installed.

Authentication type
If you leave the default setting of Server, then the Content Manager Version 8 database user ID and password is sent to the Content Manager Version 8 server for validation.

If you click Client, no validation is performed by DB2, and the user ID you type to log in to your system allows connection to the Content Manager Version 8 Library Server.

Restriction: when you log in to the client workstation, you must enter a user ID that has DB2 connect privileges.

Database connection ID
You must type the same user ID and password that was defined as the Database connection ID when the Content Manager Version 8 Library Server database was installed.

Enable sign-on
Click True to enable single sign-on, if required by your EIP system plan.

Configure Federated Server Connection

On this window, you define the information required to connect an administration client to the administration database. You see this window if you choose any connector, or if you install the administration client. EIP copies the information from this window to a configuration file named `cmbds.ini` and `cmbfedenv.ini`.

Database name
Type the administration database name.

Schema name
Type the schema name that was assigned to the administration database when the administration database was installed.

Authentication type

If you leave the default setting of Server, then the administration database user ID and password is sent to the administration database for validation.

If you click Client, no validation is performed by the database, and the user ID you type to log in to your system allows connection to the administration database.

Restriction: When you log in to the client workstation, you must enter a user ID that has DB2 connect privileges.

Database connection ID

Type the user ID and password that was defined when the administration database was installed. The user ID and password must be locally defined on the server.

Single sign-on enabled

Click to enable single sign-on, if required by your EIP system plan.

Catalog remote EIP database

Click if you want to define the remote server specifications that will enable the administration client to connect to a remote database. The remote database must be cataloged before you can connect to it. The remote EIP database catalog option is only available if you install the administration client but no local administration database.

Catalog remote database

For information on how to fill in the fields on this window, see “Connecting the administration client to a remote administration database” on page 447.

Define LDAP Server

On this window, you define the LDAP server type, hostname, port and authentication methods. EIP stores the information you type in this window in `cmbenv.properties`.

Tip: You are not required to install, configure or start any LDAP servers before you define the information required on this window.

LDAP server type

Select IBM Secureway or Microsoft Active Directory

Hostname

Type the LDAP server host name.

Port Type the LDAP server port number.

LDAP administration ID

Type the LDAP administration user ID.

Password

Type the LDAP administration password.

Destination Path for Content Manager V7 Connector C-APIs

On this window you specify the installation location for the APIs required by the Content Manager Version 7 connector. Click **Browse** to change the default path and file name.

Requirement: You must install the Content Manager Connector C-APIs on the same server where you install the administration client.

Existing Database

You see this window only if you have reused the name of an EIP database or you typed the name of a Content Manager Version 8 Library Server.

Replace the existing database?

If you click this option, DB2 drops the existing database and creates an EIP database.

Tip: If you replace the existing database, the program prompts you twice for confirmation.

Identify Administration Database

The installation program uses the information you enter on this window to connect to DB2, list the databases on the server and compare the name you define in the **Database name** field to existing databases on the server.

Tip: If you are sharing a Content Manager Version 8 database and want to verify the Content Manager Version 8 database name, or to avoid duplicating database names if you are installing a new EIP database, use DB2 Command Line Processor to list the databases on the server. Click Start→Programs-→**IBM DB2 Command Line Processor** and type `LIST DATABASE DIRECTORY` at the `db2` prompt.

If the program *does* detect a database with the same name, the program gives you the option to overwrite the database. If you are adding EIP tables to a Content Manager Version 8 database, do not overwrite the database. If the program does not detect an existing database with the same name, you are prompted to create a database. Follow the guidelines below when you define the information that identifies the administration database:

Database name

Type the administration database name. **Tip**: To avoid potential problems, do not use the special characters @, #, and $in a database name if you intend to have a client remotely connect to a host database. Also, because these characters are not common to all keyboards, do not use them if you plan to use the database in another country. Unless otherwise specified, all names can include the following characters:

- A through Z. When used in most names, characters A through Z are converted from lowercase to uppercase.
- 0 through 9
- @, #, $, and _ (underscore)

Unless otherwise specified, all names must begin with one of the following characters:

- A through Z
- @, #, and $
- If you are installing an administration or Information Mining database, accept the default database name, or type the new name.
- If you are sharing a Content Manager Version 8 Library Server database, type the Content Manager Version 8 Library Server database name that was defined when the Library Server was installed.

Schema name

- If you are installing an administration or Information Mining database, you can accept the default name, which is the same name as the Database administration ID default user ID, or change the default schema name. Type the new database name in the Schema name field. The schema name can contain up to eight letters, can contain numerals, and will appear in capital letters.
- If you are sharing a Content Manager Version 8 database, type the Content Manager Version 8 Library Server database schema name that was defined when the Library Server was installed.

A schema is a collection of named objects. A schema also provides a logical classification of objects in the database. A schema can contain objects such as aliases, tables, views, indexes, triggers, distinct types, functions, and packages. A schema can be implicitly created when an object is created. The schema exists in the database as an object. If a schema name is not specified, the first eight letters of the authorization name of the creator of the object is used as the default.

Database administration ID

The user ID and password you define in this field is used only for database creation and must be locally defined and must have DB2 administration privileges.

Restriction: You must log in to the server with a user ID that has DB2 administration privileges before you can create the administration database.

Database connection ID

The user ID and password you define in this field allows users to connect to the administration database. The user ID must be locally defined.

Image Search Server/Client Configuration

On this window, you define the Image Search server name, host name, Port number and Library Server name. EIP uses the information to locate and connect to the image search server.

Server name

Type the name of the Image Search server that was defined when the server was installed.

Host Name

Type the host name of the Image Search server. Ask the server administrator if you are required to enter a fully-qualified host name.

Port Number

Type the port number that was defined when the server was installed.

Library Server Name

Type the name of the Content Manager Version 7 Library Server database that is associated with Image Search.

Install OnDemand?

Click **Yes** or **No** when the system prompts you to confirm OnDemand client installation.

Network Table Generation (for Content Manager version 7 connector)

On this window, you click one of three options that specify information about the Content Manager Version 7 network table. When the EIP administrator defines a Content Manager Version 7 server, EIP uses the information in the network table to connect to the Content Manager Version 7 server.

Tip: The Content Manager Version 7 connector network table (`*x*:\<FRNROOT>.FRNOLINT.TBL`) and the CM for AS/400 connector network table (`*x*:\<CMBROOT>.FRNOLINT.TBL`) are separate files that have identical names.

Generate a new network table

If you click this option and click **Next**, the installation program displays a window where you enter the data required to generate `Frnolint.tbl`. EIP stores the new network table in `x:\<FRNROOT>\Frnolint.tbl`, where `x:\<FRNROOT>` is the path defined in the Destination Path for Content Manager V7 connector C-APIs window.

Copy an existing network table

If you click this option, the EIP installation program assumes that:

- `Frnolint.tbl` is already located in the path specified on the Destination Path for Content Manager V7 connector C-APIs window and
- you want to use the existing `Frnolint.tbl` without regenerating it

Generate a network table later

If you click this option, EIP installation program assumes that you plan to generate a Content Manager Version 7 network table after you install EIP. To generate a network table later, you use the program named `frnnlinc.exe`, which is installed in the path specified in the Destination Path for Content Manager V7 Connector C-API's window. EIP stores the new network table in `x:\<FRNROOT>\Frnolint.tbl`.

To use `frnnlinc.exe`:

1. Double-click `frnnlinc.exe`
2. Type `1 - Add Server Entry`.
3. Answer prompts to define server location, server type, operating system information and so forth.

Tip: You can also use `frnnlinc.exe` to Delete and Update Content Manager Version 7 server information.

Network Table Generation (for Content Manager version 7 connector)

On this window, you define the stem type, Library Server name, Port number, Host name and TP name associated with the Content Manager Version 7 library server you want to connect to.

Type Click NT, OS/2, AIX or MVS.

Server name

Type the name of the Content Manager Version 7 Library Server.

Port Number

Type the port number that was defined when the Content Manager Version 7 Library Server was installed.

Host name

Type the host name for the server where the Content Manager Version 7 Library Server was installed.

Select Administration Database Options

You see this window only if you are installing an EIP administration database that does not reuse the name of an existing administration database and you are not adding EIP tables to a Content Manager Version 8 database.

Database location
In the database location field, you specify the drive letter where the database will be installed.

Restriction: You cannot install an administration database on a remote network drive.

Enable Unicode
Click Enable Unicode if you are installing Information Mining, or an administration database to which you plan to add Information Mining tables.

Enable User Authentication from an LDAP server
Click this box to enable user authentication from an LDAP server.

Select Version of VisualInfo for AS/400

On this window, you specify the version of the VisualInfo for AS/400 server that you plan to connect to. Click Version 4.3 or Version 5.1.

Text Search Server/Client Configuration

On this window, you define the Text Search Server name, Server host name, Server Port number. When the EIP administrator defines a text search server, EIP uses the information to connect to the server.

User ID
Type the text search user ID.

Server name
Type the name of the text search server.

Server host name
Type the fully-qualified host name of the text search server.

Server port number
Type the port number assigned when the text search server was installed.

Global setting
Click **yes** or **No**.

VisualInfo for AS/400 Network Table Generation

On this window, you define the AS/400 Server name, Hostname and Port number. The information you define is copied to `x:\<CMBROOT>\frnolint.tbl`, where `x:\<CMBROOT>` is the path defined on the Specify Destination window. **Restriction:** You must install the AS/400 network table on the same drive where you install the administration client. When the EIP administrator defines an AS/400 server, EIP uses the information in `fronlint.tbl` connect to the AS/400 server.

Server Type the database name that you plan to connect to, for example, `FRNLS400`.

Hostname
Type the host name or TCP/IP address of the VI/400 server.

Tip: Ask the VI/400 administrator if you are required to enter a fully qualified Hostname.

Port Type the port number that was used to install the server.

Upgrade OnDemand?

If the installation program detects an OnDemand client on the server, EIP prompts you decide if you want to upgrade to upgrade to Version 7.1.0.2 of the OnDemand client. Click **Yes** or **No**.

After you install EIP components on Windows

Refer to “Configuring the components on Windows” on page 447 to configure the EIP components.

Chapter 13. Verifying a successful installation of Enterprise Information Portal on Windows

Use information in this section to verify a successful installation of Enterprise Information Portal on a Windows system. It includes the following procedures:

- “Verify system administration database and system administration client communication”
- “Verify Enterprise Information Portal system administration database” on page 194
- “Verify connections by running low-level connection tests” on page 195
- “Verify the installation by running Enterprise Information Portal First Steps” on page 196

Verify system administration database and system administration client communication

If the administration client and database are installed on the same server, follow the steps in this section. If the administration client and database are installed on the different Windows server, or if the database is installed on AIX or Solaris, refer to “Connecting the administration client to a remote administration database” on page 447.

Start the Enterprise Information Portal Administration Client on the Windows system in one of two ways:

Start -> Programs -> Enterprise Information Portal V8.2 -> Administration

OR

Start -> Programs -> IBM Content Manager for Multiplatforms V8.2 -> System Administration

The System Administration Client logon panel should appear. Make sure that **Enterprise Information Portal** and the correct database are selected from the drop-down lists.

Log in with icmadmin and password.

Successful logon means that your communication between the Enterprise Information Portal system administration database and the system administration client is working. It also indicates that the Enterprise Information Portal database has been created successfully (if applicable).

If you are sharing the Enterprise Information Portal database with a Content Manager library server, a successful logon means that the shared database has been configured correctly.

Once you are logged into the administration client, there is a drop-down in the upper left part of the window that you can use to switch between the interfaces for Content Manager and Enterprise Information Portal.

Test that you can see the Content Manager interface to ensure that the Content Manager connection to the system administration client is still intact.

Verify Enterprise Information Portal system administration database

Verify that the system administration database is installed correctlyas follows:

__ 1. Open a DB2 command window (**Start -> Programs -> DB2 -> Command Window**)

__ 2. Check database connection by typing:

```
db2 connect to <icmnlsdb> user <icmadmin> using <password>
```

You should see output similar to the following:

```
Database Connection Information

Database server        = DB2/NT 7.2.0
SQL authorization ID   = ICMADMIN
Local database alias   = ICMNLSDB
```

__ 3. Check database tables by typing:

```
db2 list tables
```

You should see several tables listed (around 100); some with names starting with ″FA″ (29 tables) and some starting with ″ICM″ (109 tables).

You should see several tables starting with XYZ (6 tables) added by Content Manager First Steps.

If you did not choose to use and existing database during the Enterprise Information Portal installation, you can also check `%CMBROOT%\logs\icmcrlsdb.log` and search for the term `SQLSTATE=` to find error messages. A few of the SQLSTATE messages are normal and you need to read the surrounding text to determine if there may have been a problem. For example, you should expect to find SQLSTATE=08003 messages in the log after the CONNECT RESET commands.

Verify connections by running low-level connection tests

To verify connectiona, open an Enterprise Information Portal development window:

Start -> Programs -> Enterprise Information Portal for Multiplatforms V8.2

OR

Open a DOS command window and run cmbenv81.bat

__ 1. **Test federated connector:**

```
cd %CMBROOT%\samples\java\fed
javac TConnectFed.java
java TConnectFed <icmnlsdb> <icmadmin> <password>
```

Expected output:

```
java TConnectFed icmnlsdb icmadmin password

*** connecting to datastore : icmnlsdb
*** datastore connected ***
user icmadmin dsName icmnlsdb
datastore disconnected
```

__ 2. **Test Content Manager v8 connector:**

```
cd %CMBROOT%\samples\java\icm
javac SConnectDisconnectICM.java
java SConnectDisconnectICM <icmnlsdb> <icmadmin> <password>
```

Expected output:

```
java SConnectDisconnectICM icmnlsdb icmadmin password
=======================================
IBM Enterprise Information Portal v8
Sample Program:  SConnectDisconnectICM
---------------------------------------
Database: icmnlsdb
UserName: icmadmin
=======================================
Connecting to datastore (Database 'icmnlsdb', UserName
         'icmadmin')...
Connected to datastore (Database 'icmnlsdb', UserName
         'icmadmin').
Disconnecting from datastore & destroying reference...
Disconnected from datastore & destroying reference.
==========================================
Sample program completed.
==========================================
```

Verify the installation by running Enterprise Information Portal First Steps

Enterprise Information Portal First Steps allows you to load in sample data into Enterprise Information Portal. You perform the First Steps procedures differently depending whether you have all of the Enterprise Information Portal components on one system or if you have them installed on more than one system.

If you have all of the Enterprise Information Portal components on one system, begin the first steps process in the section: "Running First Steps with Enterprise Information Portal components installed on a single machine"

If you installed the Enterprise Information Portal system administration database on another machine from your system administration client, use the procedures for First Steps in the section: "Running First Steps with Enterprise Information Portal components installed on multiple machines"

Running First Steps with Enterprise Information Portal components installed on a single machine

Start the first steps here if you installed all of the Enterprise Information Portal components on a single Windows operating system machine:

__ 1. Click **Start -> Programs -> Enterprise Information Portal V8.2 -> EIP First Steps**

__ 2. Click **Load Sample Data**. An input panel appears. The following shows the values you should enter if you selected the default values during the installation:

```
Database schema:                        ICMADMIN
User Id:                                icmadmin
Password:                               password
```

Wait several minutes for the sample databases (EIPSAMPL, XYZSAMPL, IBMPRESS) and data to be loaded. A window will pop-up with progress messages. Click **OK** once you see the message saying that the sample database has been successfully created.

__ 3. Click on **Work with Sample Data**. This will start the System administration client.

__ 4. Continue with "Validating the First Steps" on page 200

Running First Steps with Enterprise Information Portal components installed on multiple machines

Start the first steps procedure here if you installed the Enterprise Information Portal components on more than one machine, even if the components are on different operating systems:

__ 1. Ensure that the system administration client is configured to connect to a remote system administration database.

__ 2. Manually create three *sample* databases on a **remote** database machine with a DB2 Admin user ID of icmadmin, and a password of password. Create the databases as follows:

__ a.

Command:
EIP Database Install Script:

Click **Start -> Programs -> Enterprise Information Portal V8.2 -> Database Install**

OR

`c:\cmbroot\config\dbutil \eipcreatelsdb.bat`

Database name:
EIPSAMPL

Replace existing database:
Yes

Database connection ID:
ICMCONCT

LS database administrator ID:
ICMADMIN

Schema name:
ICMADMIN

Database drive:
DB2 default

Path into which the library server was installed:
`C:\Program Files\IBM\CM81`

Enable Unicode support:
Yes

Enable text search support:
Yes

Token duration time in hours:
48

Host name:
None specified (Specify if database remote)

Port number:
None specified (Specify if database remote)

Node number:
None specified (Specify if database remote)

Enable SSO support:
No

Server authentication:
Yes

__ b.

Command:
DB2 Create Database Script:

```
DB2 CREATE DATABASE IBMPRESS
USING CODESET UTF-8 TERRITORY US COLLATE
USING SYSTEM

Database name:         IBMPRESS
```

__ c.

Command:
DB2 Create Database Script:

```
DB2 CREATE DATABASE XYZSAMPL USING
CODESET UTF-8 TERRITORY US COLLATE USING
SYSTEM

Database name:         XYZSAMPL
```

__ 3. Catalog the remote databases on the local client:

__ a. Run the DB2 Client Configuration Assistant:

```
db2cca
```

or

Start -> Programs -> IBM DB2 -> Client Configuration Assistant

__ b. On the Client Configuration window: Click **Add**

__ c. On the Add Database Wizard window: click the **Source** tab, select **Search network**, and click **Next**.

__ d. On the Add Database Wizard window: click the **Database name**tab, then click **Add System**.

__ e. On the Add System window: Select **Protocol** and enter the host name

__ f. On the Add Database Wizard window: click the **Database name**tab, select **database from remote system to catalog** and click **Next**.

__ g. On the Add Database Wizard window: click the **Alias** tab, change the database alias name if needed, then click **Next**.

__ h. On the Add Database Wizard window: click the **ODBC** tab, select **register database for ODBC** and **As a system data source**; Click **Finish**.

__ i. Confirmation -<Database name> panel: Click **Test connection**

__ j. On the Connect to DB2 Database window: Enter the user ID and password used to connect to the database and click **OK**.

__ k. Repeat steps 3a through 3j for each remote database.

__ 4. Configure the EIPSAMPL remote database for use with the EIP system administration client:

__ a. Click **Start -> Programs -> Enterprise Information Portal V8.2 -> Server Configuration Utility**.

__ b. Enter the following information:

Server type:
Enterprise Information Portal

Server name:
EIPSAMPL

Schema name:
ICMADMIN

Host name:
<Host name>

Operating system:
<Operating system>

Port number:
50000 (Default DB2 port number)

Security options:
Server authentication (Default)

User ID:
icmadmin

Password:
<password>

__ 5. Click **Load Sample Data**. The following shows the values you should enter if you selected the default values during the install:

```
Database name:          EIPSAMPL
Database schema:        ICMADMIN
User Id:                icmadmin
Password:               password
```

Wait several minutes for the sample databases (EIPSAMPL, XYZSAMPL, IBMPRESS) and sample data to be loaded. A window will pop-up with progress messages. Click **OK** once you see the message saying that the sample database has been successfully created and loaded.

__ 6. Click **Work with Sample Data**. This starts the system administration client.

__ 7. Continue with "Validating the First Steps"

Validating the First Steps

__ 1. Log into the System administration client. Select **Enterprise Information Portal and EIPSAMPL**. Enter **icmadmin** and **password**.

__ 2. First Steps should connect to your EIP sample database (`EIPSAMPL`) and the samples should be loaded successfully.

__ 3. Verify that the data was loaded

Defined servers (ex. EIPSAMPL, IBMPRESS, XYZSAMPL)

Search templates (ex. SearchLongBySource, SearchXYZClaimForms)

Federated entities (ex. fed_xyz_claimforms, fed_long_article)

Chapter 14. Installing Content Manager eClient on Windows

After you have verified your Enterprise Information Portal installation, you can install the eClient.

If you are installing the eClient on the same machine that you installed Enterprise Information Portal, you do not need to install any additional prerequisites.

Before you install the eClient

Before you begin the installation process for the eClient, here are some things to consider:

- __ If you are using WebSphere Application Server (WAS) AES, stop any server that is already running on WAS. For example, if the default server is running, run `stopServer.bat` located in the `/bin` subdirectory of WebSphere. If you do not stop, then restart the IBM HTTP server, the eClient Web application cannot be installed correctly.
- __ If you are using WebSphere Application Server AE, make sure that the WebSphere Application Server administration server (AE) is running before starting the eClient installation.
- __ If you are using WebSphere Application Server 5, the application server `server 1` must be started. To start `server 1`, select **Start -> Programs -> IBM WebSphere -> Application Server v5.0 -> Start the Server**.

Installing the eClient

To install the eClient on a Windows operating system:

__ 1. Insert the eClient CD into the CD drive. The launchpad starts automatically. If the launchpad does not start automatically, execute `launchpad.bat` from the launchpad directory.

__ 2. In the launchpad, click **Install** to start the eClient installation program.

__ 3. Follow the instructions in the installation windows. The default directory for the eClient is `C:\Program Files\IBM\CMeClient`. If you are connecting to Content Manager Version 8, the default local file location of the data server list file is:

```
C:\Program Files\IBM\CMgmt\cmbicmsrvs.ini
```

__ 4. After you install the eClient files, the installation program checks for WebSphere. If the installation program detects WebSphere, you can continue with the automatic configuration of the Web application for the eClient. You can choose to exit without automatically configuring the application with WebSphere. If you choose to exit, the installation program ends, and you need to manually deploy the eClient on your Web application server.

__ 5. **Optional:**If you choose not to perform the automatic configuration, you can set up and configure the eClient as a Web application.

Validating the eClient installation

After you installed and configured the eClient as a Web application, you can verify your installation and configuration following these steps:

1. Verify that the eClient application has been deployed successfully on your WebSphere Application Server.

   For WebSphere 4.0.5 AE and WebSphere 5

   a. Open the WebSphere Application Server Administrative Console.
   b. Verify that the `eClient_Server` Application Server was created under Servers.
   c. Verify that the IBM `eClient 82` Application is installed under Enterprise Applications.

   For WebSphere 4.0.5 AES

   a. Open the WebSphere Application Server Administrative Console by clicking **Start -> Programs -> IBM WebSphere Application Server AE(s) V4.0 -> Administrator's Console**.
   b. Select **Open a configuration file to edit with the console**.
   c. Select the option, Enter full path to file on server, and enter the path to the IDM_ICM.xml configuration file located in your Content Manager Common directory (for example, `C:\Program Files\IBM\CMgmt`).
   d. In the left-hand topology frame, expand **WebSphere Administrative Domain -> Nodes ->** ***hostname*** **-> Application Servers** to find the `ICM_Server` application server.
   e. Expand **WebSphere Administrative Domain -> Nodes ->** ***hostname*** **-> Enterprise applications** to find the `IBM eClient 82` Web application.
2. Start the eClient Web application, and point your browser to

   `http://`*`hostname`*`/`*`Web application name`*`/IDMInit`

where

hostname
Name or IP address of the server machine

Web application name
Name of the eClient Web application

IDMInit
Initial connection servlet

An example of the eClient Web application address is

```
http://hostname/eClient82/IDMInit
```

If you installed the eClient correctly and the address is correct, the Logon window should open.

If you configured the eClient correctly, you should be able to access the content servers that you defined. The content servers that the eClient supports include:

- IBM Content Manager for Multiplatforms Version 7.1
- IBM Content Manager for Multiplatforms Version 8.1
- IBM Content Manager for Multiplatforms Version 8.2
- IBM Content Manager OnDemand for Multiplatforms Version 7.1
- IBM Content Manager OnDemand for OS/390 Version 2.1
- IBM Content Manager OnDemand for OS/390 Version 7.1
- IBM Content Manager OnDemand for iSeries Version 4.5
- IBM Content Manager OnDemand for iSeries Version 5.1
- IBM Content Manager ImagePlus for OS/390 Version 3.1
- IBM VisualInfo for AS/400 Version 4.3 or Version 5.1

Using the eClient with Content Manager or Enterprise Information Portal First Steps

The following steps describe an example search you can run against the sample data you loaded with **Content Manager First Steps**:

__ 1. Enter your user ID and password. Change the Server in the drop-down list to ICMNLSDB (CM8), where ICMNLSDB is the name of your Library server.

__ 2. Click **Logon**.

__ 3. Click on the Search button that appears in the eClient Home panel.

__ 4. From the Item Type List, select `XYZ_Auto` Photo.

__ 5. In the `XYZ_AdjustLName` attribute search field, enter a * (asterisk) to specify a wild card search.

__ 6. Click **Search** and the search results will be displayed to you.

__ 7. To view the associated image, click on the document icon for that item.

The following steps describe an example search you can run against the sample data you loaded with **Enterprise Information Portal First Steps**:

__ 1. Enter your user ID and password.

__ 2. Change the Server in the drop-down list to EIPSAMPL (FED). Click **Logon**.

__ 3. Click on the **Search** button that appears in the eClient Home window.

__ 4. From the Templates listed, select **SearchXYZClaimForms**.

__ 5. In the **Last name** search field, enter: `Twain`

__ 6. Click **Search** and the search results will be displayed to you.

IMPORTANT: For IMPORT capability, you will need to modify the IDM.properties file. Change the ImportEnabled value from False to True. You need to make similar modifications for other capabilities such as check-in and check-out, e-mail, re-indexing, create folder, etc. See the *Installing, Configuring, and Managing the eClient* document for further details.

Chapter 15. Installing the Content Manager Client for Windows

This section provides the information for installing the Content Manager Client for Windows. It is not necessary to uninstall an earlier version of the Client for Windows program before you begin.

Before you begin

Before you begin the installation, meet with your system administrator to plan for and obtain information that you need during the Client for Windows installation. You need know where your Initialization (configuration) files will be located. Decide on one of the following:

- On a remote http location:_________________________
- On a remote ″mapped″ network location:__________________
- On this workstation (Local)

  If the initialization files will be located on this workstation, you need to understand/plan for information in the following two charts:

Initialization file information	**Record values here**
Datastore alias name	
DB2 user ID	
DB2 password	
DB2 schema name	
Database location: **remote** or **local**.	
Authentication: related to DB2 database manager authentication. Choose **Client** or **Server**.	
Single sign-on: this option is only available when you choose **Client** (above).	

Remote database catalog information	**Record values here**
Host name of database server	
Port number (of the remote database)	
Remote database name	
Database node name	

Remote database catalog information	Record values here
The platform of the system (where the remote database is located):	

For more information about initialization (ini) files, see Chapter 34, “Generating configuration files”, on page 515.

Beginning the installation

To begin the installation, complete the following steps:

__ 1. Shut down any open Windows applications, including antivirus software.

__ 2. Insert the Client for Windows CD in your CD-ROM drive. If the ″Choose setup Language″ window opens automatically, go to step 3.

If the ″Choose setup Language″ window does not open automatically, start the setup program manually, for example:

a. Click **Start** → **Run**

b. Enter `[x]:\setup.exe`, where [x] is the designation of your CD drive.

__ 3. Select the language that you want to use during the installation program. Here are some things that you need to consider when you choose the language:

- When you choose the language to run during the installation program, you can install the Client for Windows in another or several other languages. For example: you can select French to start the installation, then later in the installation, select to install the English and German versions of the Client for Windows.
- The language that you choose to start the installation affects the language that is used to install the DB2 runtime client. To select another language for the DB2 runtime client, you need to uninstall the runtime client, then reinstall it from the Client for Windows CD and select the other language that you want to use.

Click **OK**.

__ 4. When the Welcome window opens, click **Next**.

__ 5. The Destination Folder window opens. To accept the default location for installing the Client for Windows program, click **Next**.

If you want to install the Client for Windows program in a different location, click **Change**, select the location that you want, then click **OK**.

Note: If you have a previous version of the product on this workstation, the installation program **does not** use that location for the Client for Windows program. It is intended that you be able to have both a Version 8 and a Version 7.2 Client installed and operable (concurrently).

__ 6. The Setup Type Selection window opens. Select the type of installation that you want to run:

Typical
This selection does not install all possible components. It installs all components **except for**:

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

Custom
To select specific components.

Click **Next**, and go to step 8 on page 208 if you choose **Typical**, or step 7 for **Custom** options.

__ 7. You can choose from the following components in the Custom Setup window:

Client Application
Install the Client Application to work with documents and folders in the Content Manager system.

This component contains the Scanner support sub-component. You must select it to install it.

Languages
Choose the languages that you want to have installed. You can choose more than one language (for the Client for Windows only).

ODMA
Install ODMA support if you want to be able to access documents stored in a Content Manager system directly from certain workstation applications.

Note about ODMA:
ODMA installs only in the same language that the install program runs in. However, ODMA is not translated into the following languages: Czech, Danish, Dutch, Hebrew, Hungarian, Norwegian, Polish, Russian, Slovakian, Sovenian, or Swedish.

When you install in one of these languages, you get English ODMA. Only some internal messages will be translated.

__ 8. The ″Content Manager Initialization Files Location - Remote″ window opens.

Important

> This is the point in the install that you need to refer to the planning information that you prepared at the beginning of this section.

If your initialization files are located (or will be located in the future) on a remote http server, enter the URL address here, then click **Next** and go to step 11.

If your initialization files are **not** (or will not be) located on a remote http server, leave it blank, then click **Next**.

__ 9. The ″Initialization Files Location - Local″ window opens. Specify the location of your local folder for the initialization files, then click **Next**.

__ 10. Enter the requested information using the information you gathered at the beginning of this section.

Hint: It is best if you have the correct information at this time. If you do not have it, you have two options:

- You can skip entering the initialization information (by clicking the **Skip for now** button), and continue with the installation. (You can modify the initialization files later.)
- You can cancel the installation program and run it at a later time when you have the information.

  This is the **recommended** option.

__ 11. When the Ready to Install window opens, click **Install** to begin copying files to your workstation.

Validating the installation

Use the following steps to validate the Client for Windows installation:

__ 1. Launch the Client for Windows. Go to **Start -> Programs -> IBM Content Manager V8 -> Client for Windows**

__ 2. Login to your Content Manager Library Server using the Client for Windows.

The following steps describe an example search you can run against the sample data you loaded with CM First Steps:

__ 1. Click on the **Search** button that appears in the Welcome panel.

__ 2. From the **Item Type** drop-down list, select **Auto Photo** (Content Manager V8 Sample Item Type).

__ 3. In the **Adjuster Last Name** attribute search field, enter a * (asterisk) to specify a wild card search.

__ 4. Click **OK** and the search results will be displayed to you.

__ 5. To view the associated image, double-click on the item.

Part 3. Installing Content Manager on an AIX operating system

This section contains information needed to install and configure the IBM Content Manager and Enterprise Information Portal software on the AIX operating system. The information in this section is based on the steps identified using the *Planning Assistant* from the *Start Here CD*.

The prerequisite and installation details in this section are presented in the required order of installation. All steps are presented as if each one is required on this single workstation (for a single server configuration). In fact, you may only need some of the steps, depending on your own configuration needs:

1. Chapter 16, “Installing and updating prerequisite programs for AIX”, on page 213
2. Chapter 17, “Performing pre-installation steps on AIX”, on page 235
3. Chapter 18, “Installing Content Manager components on AIX”, on page 245
4. Chapter 19, “Verifying a successful installation of Content Manager on AIX”, on page 281
5. Chapter 20, “Installing Enterprise Information Portal components on AIX”, on page 305
6. Chapter 21, “Verifying a successful installation of Enterprise Information Portal on AIX”, on page 315
7. Chapter 22, “Installing the Content Manager eClient on AIX”, on page 319

Chapter 16. Installing and updating prerequisite programs for AIX

This section has two sub-sections:

1. "Verifying your software Prerequisites on AIX" explains how to check the level of a prerequisite that you already have installed on your system.
2. "Installing or Updating Prerequisite programs" on page 215 has detailed instructions for how to install and configure the prerequisite programs that are needed for your own planned configuration.
   - The steps that you need to perform are determined by the selections that you make while you are using the ″Planning Assistant″ from the *Start Here CD*.
   - The planning assistant produces output sheets (with checklists) for the programs and components that you need to install for your selected components.

   The prerequisite programs included in this section are:
   - "AIX operating system" on page 215
   - "IBM VisualAge C++ Professional Batch compiler" on page 216
   - "IBM DB2 Universal Database" on page 217
   - "Oracle database on an AIX system" on page 222
   - "IBM DB2 Net Search Extender (NSE) and Text Information Extender (TIE)" on page 227
   - "IBM WebSphere Application Server (WAS)" on page 228

Verifying your software Prerequisites on AIX

Run the following verification checks to determine which of the prerequisites you need to install or update. For those prerequisites that are either not installed or at the expected level, use the next section ("Installing or Updating Prerequisite programs" on page 215) to guide you through installing them.

Table 74. Basic prerequisite verification

Prerequisite	How to check	Expected value
1. AIX 4.3.3 ML 9 + or higher + APAR IY19277 2. AIX 5.1 ML 1	`oslevel -r`	1. 4330-09 or higher 2. 5100-01 or higher

Table 74. Basic prerequisite verification (continued)

Prerequisite	How to check	Expected value

IBM VisualAge C++ Batch Compiler ver. 5.0.2.0 On AIX 5.1 you need ptfs IY18426 and IY23677.	`lslpp -l | grep vacpp`	level#: 5.0.2.0 or higher Component examples:
		`vacpp.cmp.batch`
		`vacpp.cmp.rte`

Visual Age C++ Professional batch compiler for AIX Version 5.0.2.0 or higher	`lslpp -L vacpp.cmp.batch`	Level: 5.0.2.0 or higher

DB2 UDB ver 8.1	`lslpp -l | grep db2`	level#: 8.1.1.0 Component examples:
		`db2_08_01.adt.rte`
		`db2_08_01.das`
		`db2_08_01.db2.rte`

DB2 UDB Enterprise Extended Edition Version 7.2 with Fixpack 7 or higher	From the DB2 Command Window: `db2level`	Level needs to read ″SQL07025″ or greater with fixpack level of ″WR21306″ or greater.
DB2 UDB Enterprise Server Edition Version 8.1 with Fixpack 1	From the DB2 Command Window: `db2level`	Level needs to read SQL08010 or read ″DB2 v8.1.1.27″. The fixpack information needs to read ″FixPak ″1″″ and list the fixpack level, for example, ″s021124″ is the fixpack that had been available November 24, 2002. For Oracle, the fixpack level must be S021110 or later.
DB2 Text Information Extender v7.2 fp 1	`lslpp -l | grep db2tie`	level#: 7.2.0.1 Component examples: `db2_07_01.db2tie`

DB2 Net Search Extender (required if you use DB2 Version 8.1)	From the DB2 Command Window, start the text search program:
	`db2text start`
	Then type:
	`db2textlevel`
		CTE0350 Instance ″DB2″ uses DB2 Net Search Extender code release ″ tx9_81″ with level identifier″ tx9_26a″

Tivoli Storage Manager API Client Version 4.2.1	`/opt/tivoli/tsm/client/api/samprun`	API Library Version = 4.2.1.0

Table 74. Basic prerequisite verification (continued)

Prerequisite	How to check	Expected value
Tivoli Storage Manager Server Version 4.2.1	Logon to the TSM Server Administration web page: `http://<hostname>:1580` Where `<hostname>` is the name of the TSM server.	The version appears on the Web page. It should say Version 4, Release2, Level1.0
1. WebSphere AppServer AE 2. WebSphere AppServer AES - v4.0.5	`grep "<version>" /usr/WebSphere/AppServer /properties/com/ibm /websphere/product.xml`	<version>**4.0.5**</version>u

Table 75. Prerequisite verification for Oracle

Prerequisite	How to check	Expected value
DB2 Relational Connect Version 8.1 with fixpack 1	From a DB2 Command Window: db2level	Level: s021110 or later
Oracle Version 8.1.7.4 or Version 9.2.0.1	Connect to an existing Oracle database: `Squlplus userID/user_password@ databasename.domainname`	Oracle 8i Enterprise Edition 8.1.7.4.0 PL/SQL 8.1.7.4.0 TNS for 32-bit Windows: 8.1.7.4.0
	To check the version type: `select * from product_component_version;`	Oracle 9i Enterprise Edition 9.2.0.1 PL/SQL 9.2.0.1 TNS for 32-bit Windows: 9.2.0.1

Installing or Updating Prerequisite programs

This section guides you through installing each of the prerequisite programs for Content Manager.

The rule of thumb when installing the prerequisites is to always apply the fixpacks after your base components are installed. For instance, if you are missing the DB2 UDB Application Development Client from your DB2 install, install this component first, then install the fixpack code. Otherwise, you will need to install the fixpack code again after adding any new DB2 components.

AIX operating system

One of the following AIX operating systems is required for Content Manager, Version 8 Release 2:

- AIX 4.3.3 with maintenance level 9 or later
- AIX 5.1 with maintenance level 1 or later

Your system should already be at AIX 4.3.3 or AIX 5.1.

- To download maintenance level 9 for AIX 4.3.3, go to the following website:

  http://techsupport.services.ibm.com/server/mlfixes/43
- To download maintenance level 1 for AIX 5.1, go to the following website:

  http://techsupport.services.ibm.com/server/aix.fdc51?
  toggle=DNLDML

Follow the Download and Install instructions provided at the AIX download site. Reboot your system after you have installed the updates.

To **validate** that your system is at the correct level, re-run the oslevel command:

```
oslevel -r
```

You should see the following output:

```
4330-09
```

IBM VisualAge C++ Professional Batch compiler

You must have IBM VisualAge C++ Professional Batch compiler, version 5.0.2.0 or later to run the Content Manager, Version 8 Release 2 library server.

Where to obtain the IBM Visual Age C++ compiler program program

Two possible methods for obtaining the IBM Visual Age C++ compiler program are:

- You can work with your IBM sales representative to obtain it
- You can download a trial version of the program

You can download a **60 day try & buy** version of the VisualAge C++ compiler at the following location:

http://www.ibm.com/software/ad/vacpp/

__ 1. Select ″VisualAge C++ Professional for AIX5.0, try it for 60 days!″

__ 2. Complete the registration information

To **download fixes**:

- either to get you to level 5.0.2.0
- or, for the ptfs **IY18426** and **IY23677** that are needed or AIX version 5.1

Go to the same vacpp website (repeated here):

http://www.ibm.com/software/ad/vacpp/

and complete these steps:

__ 1. Select **Downloads** in the left panel.

__ 2. Limit you search by selecting:

  - platform/operating system: **AIX**

- version: **5.0**

__ 3. In the Search entry field enter 5.0.2.0 or the ptf names to identify the download packages for the fix you need.

How to install or upgrade IBM Visual Age C++ compiler

To install IBM Visual Age C++, follow the installation instructions that come with the program code.

Use the System Management utility to install IBM VisualAge C++ software, for example, you can use **smitty**:

- Select **Software Installation and Maintenance**
- Select **Install and Update Software**
- Select **Install and Update from LATEST Available Software**
- On the Install window, enter the directory which contains the IBM Visual Age C++ code next to: *** INPUT device/directory for software**
- Check all the options on the ″Install″ screen and make sure all the values are correct.
- Press **enter** and a confirmation dialog appears to ask you to confirm the installation.

How to validate your IBM Visual Age C++ installation

To validate your IBM Visual Age C++ installation, re-run the lslpp command:

```
lslpp -l vacpp.cmp*
```

You should see the following output:

```
vacpp.cmp.C            5.0.2.0  COMMITTED  VisualAge C++ C Compiler
vacpp.cmp.aix43.lib    5.0.2.0  COMMITTED  VisualAge C++ Libraries
                                                          for AIX 4.3
vacpp.cmp.batch        5.0.2.0  COMMITTED  VisualAge C++ Batch Compiler
vacpp.cmp.core         5.0.2.0  COMMITTED  VisualAge C++ Compiler
vacpp.cmp.extension    5.0.2.0  COMMITTED  VisualAge C++ Extension Interface
vacpp.cmp.include      5.0.2.0  COMMITTED  VisualAge C++ Compiler
                                                         Include Files
vacpp.cmp.incremental  5.0.2.0  COMMITTED  VisualAge C++ Incremental
                                                              Compiler
vacpp.cmp.lib          5.0.2.0  COMMITTED  VisualAge C++ Libraries
vacpp.cmp.rte          5.0.2.0  COMMITTED  VisualAge C++ Compiler
                                                     Application Runtime
vacpp.cmp.tools        5.0.2.0  COMMITTED  VisualAge C++ Tools
```

IBM DB2 Universal Database

IBM DB2 Universal Database Enterprise Edition Version 7.2 OR Enterprise Extended Edition Version 7.2.1. (or higher) is required for Content Manager Version 8 Release 2 servers when you use DB2 for your server databases. IBM DB2 Universal Database Enterprise Server Edition Version 8.1 is required when you use Oracle for your server databases. IBM DB2 Universal Database Enterprise Server Edition Version 8.1 (at fixpack 1 code level) is included in the Content Manager package.

If you are planning to use a DB2 database for your library server and resource manager, continue with this section to install IBM DB2 Universal Database Enterprise Server Edition Version 8.1 (included in the Content Manager package).

If you are planning to use an Oracle database with your Content Manager library server and resource manager, use the instructions for installing DB2 Universal Database and DB2 Relational Connect that are provided in the section: "Oracle database on an AIX system" on page 222.

Before you begin to install IBM DB2 Universal Database

Before you begin to install IBM DB2 Universal Database, complete the following steps:

__ 1. Ensure that your machine has enough memory and disk space for your installation. See the DB2 product documentation on the DB2 Online Support Web site for the requirements at:

   www.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8pubs.d2w/en_main

__ 2. Make sure that you do not have a previous version of DB2 already installed on the machine. If a previous version of DB2 is installed, you need to migrate servers and instances, depending on the version installed. In this case, do not follow these instructions. Instead, refer to the DB2 product documentation on the DB2 Online Support Web site at:

   www.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8pubs.d2w/en_main

__ 3. Your DB2 database server will reside on the same machine as WebSphere Application Server. This configuration and the use of the default settings documented in these instructions are appropriate only for development and small production environments. For larger environments where it is preferable to configure the DB2 server on a remote machine, you must install and configure a DB2 client on the same machine on which you install WebSphere Application Server and verify the remote database connectivity. See the IBM Redbook, *WebSphere V3.5 Handbook*, on the IBM Redbooks Web site at:

   www.redbooks.ibm.com/redbooks/SG246161.html

   for more information about implementing this configuration.

Important: Install DB2 before installing WebSphere Application Server.

__ 4. The DB2 CD in the package may contain a compressed image. You may have to untar it before you use it.

Installing IBM DB2 Universal Database

Perform the following steps to install DB2:

__ 1. Ensure that you are logged into the machine with super user (root) privileges.

__ 2. Ensure that a CD-ROM drive is installed and configured on the machine. If a CD-ROM drive is not installed or configured on the machine, install and configure one according to the instructions provided with the drive.

__ 3. Insert the DB2 UDB V8.1 CD-ROM into the CD-ROM drive.

__ 4. If necessary, use the mkdir command to create a mount point for the CD-ROM. The following command creates a mount point at the directory /cdrom; you can mount the CD-ROM at any location on the machine's local file system.

```
# mkdir /cdrom
```

The commands in these steps assume the CD-ROM is mounted at /cdrom. If you mount the CD-ROM at a different location, use that location when issuing commands.

__ 5. Mount the CD-ROM drive by entering the following command:

```
# mount -o ro -v cdrfs /dev/cdnumber /cdrom
```

In this command, `number` is the CD-ROM number for your system, usually 0 (zero). Note that this command assumes that the CD-ROM is mounted at `/cdrom`.

__ 6. Navigate to the /cdrom directory.

__ 7. Start the DB2 installation by invoking the DB2 Setup Utility (db2setup) as follows:

```
# ./db2setup
```

__ 8. From the IBM DB2 Setup Launchpad (Welcome) window, you can view installation prerequisites and the release notes. You may want to review the installation prerequisites and release notes for late-breaking information. Click **Install Products** to begin the installation.

__ 9. The Setup window opens. Select DB2 UDB Enterprise ServerEdition, then click **Next**.

__ 10. Once you have initiated the installation, proceed by following the setup program's prompts.

When prompted, select **Typical** as the installation type, to install all DB2 components required to support Content Manager. You can take most default options (unless you have specific requirements of your own).

Online help is available to guide you through the remaining steps. To invoke the online help, click **Help** or press **F1**. You can click **Cancel** at any time to end the installation. DB2 files will only be copied to your computer once you have clicked **Finish** on the last DB2 Setup wizard installation panel.

__ 11. Unmount the CD-ROM before removing it from the CD-ROM drive by using the **umount** command, as follows:

```
# umount /cdrom
```

Steps to complete after installing DB2 and before installing Content Manager

After you install DB2 perform the following steps for Content Manager:

__ 1. Ensure that the user named root is a member of the group set named **db2grp1** by performing the following steps:

  __ a. Invoke SMIT to change characteristics of a user by entering the following command:

  ```
  # smit chuser
  ```

  The Change/Show Characteristics of a User dialog box opens.

  __ b. In the **User NAME** field, type `root` and press **Return**.

  __ c. In the **GROUP SET** field, ensure that the group db2grp1 is listed. If it is not, append it to the list of groups, and press **Return**.

  __ d. When the process is complete, exit from SMIT.

__ 2. Create symbolic links from the home directory of the instance owner to the DB2 installation directory by executing the db2ln script, as follows:

```
# /usr/opt/db2_08_01/cfg/db2ln
```

__ 3. Configure the user `root` to run the db2profile or db2cshrc at login:

- For the Korn shell (ksh), add the following text to the /.profile file of root. Note the space between the period (.) and the first slash (/).

  ```
  . /home/db2inst1/sqllib/db2profile
  ```

- For the C shell (csh), add the following line to the `/.cshrc` file of root:

  ```
  source /home/db2inst1/sqllib/db2cshrc
  ```

  Log out then log back in for your changes to take effect.

Configuring the database manager to use shared memory

Before starting DB2 on AIX you must configure the database manager to use extended shared memory, as follows:

__ 1. Log in as the DB2 instance owner, **db2inst1**, by using the **su** command, as follows:

```
# su - db2inst1
```

When you log in as db2inst1, the command prompt changes from the # symbol to a dollar sign ($) to indicate a change in your login identity.

__ 2. If this is the first time that you have logged in as the DB2 instance owner, you could be prompted to change the password. Enter a new password and press Return. DB2 requires a password of eight or fewer characters.

__ 3. When prompted, type the new password again and press **Return**.

__ 4. Set the EXTSHM environment variable by entering the following commands:

```
$ EXTSHM=ON
$ export EXTSHM
$ db2set DB2ENVLIST=EXTSHM
```

Ensure: that the EXTSHM environment variable is set each time you start DB2. Do this by editing `/home/db2inst1/sqllib/profile.env` and add or modify the line:

```
DB2ENVLIST='EXTSHM'
```

Also add the following to `/home/db2inst1/sqllib/userprofile`:

```
export EXTSHM=ON
```

Validating the IBM DB2 Universal Database installation

To demonstrate that DB2 is functioning correctly, you can create a sample database and compile and execute a Java application that accesses it. You can see that the environment is set up correctly for DB2 and for IBM Java 2 SDK, and that the JDBC provider is accessible from a Java application.

Perform the following steps to create the sample database and compile and run the Java application:

__ 1. Ensure that you are logged in as the DB2 instance owner, **db2inst1**.

__ 2. Ensure that the DB2 environment has been set up correctly by using the echo command to verify the value of the DB2INSTANCE environment variable, as follows:

```
 $ echo $DB2INSTANCE
```

The correct value returned is **db2inst1**.

__ 3. Ensure that the home directory of the instance owner, /home/db2inst1, has write permissions.

__ 4. Create the sample database by executing the db2sampl script, as follows:

```
$ db2sampl
```

This process can take several minutes to complete.

__ 5. Ensure that you are in the instance owner's home directory, /home/db2inst1.

__ 6. Compile an example Java application by using the javac command, as follows:

```
$ javac -d . sqllib/samples/java/DB2Appl.java
```

The resulting class file is created in the local directory.

__ 7. Start DB2 by using the db2start command, as follows:

```
$ db2start
```

__ 8. Run the Java sample by using the java command, as follows:

```
$ java DB2Appl
```

Correct output resembles the following:

```
Retrieve some data from the database...
Received results:
empno= 000010 firstname= CHRISTINE
empno= 000020 firstname= MICHAEL
empno= 000030 firstname= SALLY
. . .
Update the database...
Changed 1 row.
```

For a final verification, type the command

```
# db2level
```

You should see data that is similar to the following:

```
DB21085I Instance "db2inst1" uses DB2 code release "SQL08010"
 with level identifier "01010106".
Informational tokens are "DB2 v8.1.1.0", "s021023", "" and FixPak "0".
Product is installed at "/usr/opt/db2_08_01".
```

Oracle database on an AIX system

This section helps you set up the required prerequisite programs if you want to access Oracle data sources for your library server. Depending on your planned configuration, you will be installing the following software:

For the library server database component

- Oracle Enterprise server software, Version 8.1.7.4 OR Version 9.2.0.1 or later

- IBM DB2 Universal Database Enterprise Server Edition Version 8.1 with fixpack 1 applied (s021110 or later)
- DB2 Relational Connect Version 8.1 with fixpack 1 applied (s021110 or later)

For the library server application component

If the library server application component is going to be installed on the same machine as the library server database component:

- Oracle Enterprise server software, Version 8.1.7.4 OR Version 9.2.0.1 or later
- IBM DB2 Universal Database Enterprise Server Edition Version 8.1 with fixpack 1 applied (s021110 or later)
- DB2 Relational Connect Version 8.1 with fixpack 1 applied (s021110 or later)

If the library server database component is going to be installed on a remote Oracle server machine from the library server application component:

- Oracle Enterprise client software, Version 8.1.7.4 OR Version 9.2.0.1 or later

Before you begin to install the Oracle server or client software

Before you begin to install IBM DB2 Universal Database, ensure that your machine has enough memory and disk space for the installation, and that you meet all the requirements for the installation. See the following Oracle web site for the platform-specific requirements:

http://technet.oracle.com

Installing the Oracle server software for the library server database component

To install Oracle Enterprise Edition server software, Version 8.1.7.4 OR Version 9.2.0.1 (or later):

__ 1. Log on to the system as a user ID that has root authority.

__ 2. Use the installation procedures in the documentation that comes with the Oracle software for details on how to install the Oracle server software.

Installing the Oracle client software for a remote library server application component

To install Oracle Enterprise Edition client software, Version 8.1.7.4 OR Version 9.2.0.1 (or later):

__ 1. Log on to the system as a user ID that has root authority.

__ 2. Use the installation procedures in the documentation that comes with the Oracle software for details on how to install the Oracle client software. Become aware of any compatibility issues between different levels of Oracle client software and Oracle server software by consulting Oracle documentation, the Oracle TechNet website, the Oracle Metalink website, or Oracle customer service.

__ 3. To ensure that the client software is able to connect to the Oracle server, use the Oracle **sqlplus** tool to connect to an existing database on the Oracle server.

You should see the following fields in your `sqlnet.ora` file in your `ORACLE_HOME/NETWORK/ADMIN` directory:

```
SQLNET.AUTHENTICATION_SERVICES=(NTS)
NAMES.DIRECTORY_PATH= (TSNAMES,ONAMES,HOSTNAME)
```

Before you begin to install IBM DB2 Universal Database

Before you begin to install IBM DB2 Universal Database, complete the following steps:

__ 1. Ensure that your machine has enough memory and disk space for your installation. See the DB2 product documentation on the DB2 Online Support Web site for the requirements at:

www.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8pubs.d2w/en_main

__ 2. Make sure that you do not have a previous version of DB2 already installed on the machine. If a previous version of DB2 is installed, you need to migrate servers and instances, depending on the version installed. In this case, do not follow these instructions. Instead, refer to the DB2 product documentation on the DB2 Online Support Web site at:

www.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8pubs.d2w/en_main

__ 3. Your DB2 database server will reside on the same machine as WebSphere Application Server. This configuration and the use of the default settings documented in these instructions are appropriate only for development and small production environments. For larger environments where it is preferable to configure the DB2 server on a remote machine, you must install and configure a DB2 client on the same machine on which you install WebSphere Application Server and verify the remote database connectivity. See the IBM Redbook, *WebSphere V3.5 Handbook*, on the IBM Redbooks Web site at:

www.redbooks.ibm.com/redbooks/SG246161.html

for more information about implementing this configuration.

Important: Install DB2 before installing WebSphere Application Server.

__ 4. The DB2 CD in the package may contain a compressed image for DB2 ESE and for DB2 Relational Connect. Your may have to untar it before you use it.

Installing IBM DB2 Universal Database Enterprise Server Edition

To Install IBM DB2 Enterprise Server Edition:

__ 1. Insert the DB2 UDB V8.1 CD-ROM into the CD-ROM drive.

__ 2. If necessary, use the mkdir command to create a mount point for the CD-ROM. The following command creates a mount point at the directory /cdrom; you can mount the CD-ROM at any location on the machine's local file system.

```
  # mkdir /cdrom
```

The commands in these steps assume the CD-ROM is mounted at /cdrom. If you mount the CD-ROM at a different location, use that location when issuing commands.

__ 3. Mount the CD-ROM drive by entering the following command:

```
# mount -o ro -v cdrfs /dev/cdnumber /cdrom
```

In this command, `number` is the CD-ROM number for your system, usually 0 (zero). Note that this command assumes that the CD-ROM is mounted at `/cdrom`.

__ 4. Navigate to the /cdrom directory.

__ 5. Start the DB2 installation by invoking the DB2 Setup Utility (db2setup) as follows:

```
# ./db2setup
```

__ 6. From the IBM DB2 Setup Launchpad (Welcome) window, you can view installation prerequisites and the release notes. You may want to review the installation prerequisites and release notes for late-breaking information. Click **Install Products** to begin the installation.

__ 7. Proceed through the DB2 Setup Wizard installation panels and make your selections.

Note: As part of the installation, do not create a DB2 instance. You will create the instance when you install DB2 Relational Connect.

Installation help is available to guide you through the steps. To invoke the installation help, click Help or press F1. You can click Cancel at any time to end the installation.

__ 8. Click Finish on the last DB2 Setup Wizard installation panel to copy the DB2 files to your system.

When you complete the installation, DB2 is installed in the following directory:`/usr/opt/db2_08_01`

Installing IBM DB2 Universal Database Relational Connect

After you install the client software and the DB2 server software, you need to install DB2 Relational Connect, Version 8 on the DB2 server. DB2 Relational Connect contains the software that you need to access Oracle data sources.

__ 1. Log on to the system under a user ID that has root authority.

__ 2. Close all open programs so that the installation program can update files as required.

__ 3. Insert the DB2 Relational Connect CD, and start the setup program to install DB2 Relational Connect.

__ 4. If necessary, use the mkdir command to create a mount point for the CD-ROM. The following command creates a mount point at the directory /cdrom; you can mount the CD-ROM at any location on the machine's local file system.

```
  # mkdir /cdrom
```

The commands in these steps assume the CD-ROM is mounted at /cdrom. If you mount the CD-ROM at a different location, use that location when issuing commands.

__ 5. Mount the CD-ROM drive by entering the following command:

```
# mount -o ro -v cdrfs /dev/cdnumber /cdrom
```

In this command, `number` is the CD-ROM number for your system, usually 0 (zero). Note that this command assumes that the CD-ROM is mounted at `/cdrom`.

__ 6. Navigate to the /cdrom directory.

__ 7. Start the DB2 Relational Connect installation by invoking the DB2 Setup Utility (db2setup) as follows:

```
# ./db2setup
```

__ 8. The DB2 Relational Connect Setup Launchpad opens. From this window review the installation prerequisites and release notes for late-breaking setup information.

__ 9. From the Select the features to install panel in the setup program, choose **Relational Connect for Oracle Data Sources**. The set up will require you to identify the local path where you installed the Oracle client software.

The Relational Connect installation will update the `sqllib/cfg/db2dj.ini` file to set the ORACLE_HOME environment variable. If you need to set the ORACLE_BASE and ORA_NLS environment variables, you will need to set them manually.

The installation will also link DB2 to the Oracle client software.

Caution: If you do not install the Oracle client software before you run the DB2 Relational Connect installation, you will have to manually set the environment variables and link DB2 to the client software.

Installation help is available to guide you through the steps. To invoke the installation help, click **Help** or press F1. You can click Cancel at any time to end the installation.

__ 10. As part of the installation:

- Create a DB2 instance on the federated server. This will set the DB2 database manager FEDERATED parameter to YES, which enables the DB2 server to access the data sources.
- Specify the user authorities information for the instance.

__ 11. Click **Finish** on the last setup installation panel to copy the DB2 Relational Connect files to your system.

When you complete the installation, DB2 Relational Connect is installed in the same directory as the DB2 server software.

IBM DB2 Net Search Extender (NSE) and Text Information Extender (TIE)

The powerful text search capabilities of the DB2 Version 7 Text Information Extender (TIE) are merged into the Net Search Extender (NSE) Version 8. Notice that if you plan to use the (optional) text search feature of Content Manager, you must install:

IBM Text Information Extender (TIE), Version 7.2 with IBM DB2 Enterprise Edition Version 7.2 and Enterprise Extended Edition Version 7.2.1

OR

IBM Net Search Extender (NSE), Version 8 with IBM DB2 Enterprise Server Edition, Version 8.1.

IBM Net Search Extender (NSE), Version 8 is provided in the package with Content Manager, Version 8.2.

Installing IBM DB2 NSE

Refer to the installation instructions on the documentation CD supplied with DB2 Net Search Extender (NSE).

NSE must be installed on the same workstation as the library server.

Validating the DB2 NSE installation

To verify proper NSE installation, make sure DB2 is started and execute the following command to start DB2 NSE:

```
# db2start
# db2text start
```

You should see the following output:

```
CTE0001 Operation completed successfully.
```

IBM WebSphere Application Server (WAS)

IBM WebSphere Application Server, Version 5 is provided in this package with Content ManagerVersion 8.2. It includes:

- IBM HTTP Server
- Java Development Kit (JDK)

Installing IBM WebSphere Application Server

Use this section to install IBM WebSphere Application Server:

__ 1. Go to the WebSphere 5.0 InfoCenter online documentation for your configuration of the Application Server and in your language at:

http://www.ibm.com/software/webservers/appserv/infocenter.html

__ 2. Under the section entitled ″Version 5 InfoCenters:″, select your language in the drop-down box next to **Application Server for distributed operating systems**.

__ 3. Expand **Getting Started -> Installing WebSphere Application Server -> Installing the product** in the left navigation panel of the WebSphere InfoCenter

__ 4. Follow the instructions in the right panel for installing WebSphere as it applies to your operating system.

Validate the installation

To validate the WebSphere installation, use the information under **Getting Started -> Installing WebSphere Application Server -> Using the installation verification steps** in the WebSphere InfoCenter (that you opened during the installation steps above).

Installing MQSeries Workflow for AIX

You can install MQSeries for AIX Version 5.2 on any server that can run AIX Version 4.2.

Installing MQSeries on AIX

Before you can install MQSeries for AIX you must create and mount a `/var/mqm` file system, or `/var/mqm`, `/var/mqm/log`, and `/var/mqm/errors` file systems.

Allow a minimum of 30 MB of storage for `/var/mqm`, 2 MB of storage for `/var/mqm/errors`, and 20 MB of storage for `/var/mqm/log` if you choose to create separate file systems.

To use SMIT for the installation,

- Log in to SMIT with `root` authority. From the shell, type: `smit`

- Select the appropriate device appropriate for your installation using this sequence of windows:
  - Software Installation and Maintenance
  - Install and Update Software
  - Install and Update from LATEST Available Software

You can also use the alternative fast path command:

- `smitty install_latest`

Press **List** to display the Single Select List window.

Select: `/dev/cd0 (CD-ROM Drive)`Select **Do** to display the parameters for Install Latest Level.

Press **F4** to obtain a list of components to install.

Press **Enter.**

If you have a previous version of the product on your machine, change the Auto Install prerequisite software to **No** and Overwrite existing version to **Yes**.

Select **Do** to install the software.

Tip: if you want to verify as root, you must add **Root** to the **mqm** group

MQSeries AIX installation verification procedures

This section describes how to verify a local (standalone) installation, involving no communication links to other MQSeries machines.

Follow the steps in this section to install and test a simple configuration of one queue manager and one queue. In this process, you use sample applications to put a message onto the queue and to read the message from the queue.

1. Install MQSeries for AIX on the workstation (include the Base Server component as a minimum).
2. Create a default queue manager (in this example called `venus.queue.manager`):
   a. At the command prompt in the window type: `crtmqm -q venus.queue.manager`
   b. Press **Enter.** Messages are displayed telling you that the queue manager has been created, and that the default MQSeries objects have been created.

Tip: In prior releases of MQSeries, it was necessary to run a script file called amqscoma.tst to define the MQSeries default objects. This step is not required in this release of the product.

3. Start the default queue manager:
   - Type strmqm and then press **Enter**:
   - A message tells you when the queue manager starts.
4. To enable MQSC commands, type runmqsc and press **Enter**.

   Tip: MQSC has started when the following message appears: Starting MQSeries Commands. MSQC has no command prompt.
5. Define a local queue (in this example, called ORANGE.QUEUE):
   - Type define qlocal (orange.queue). and press Enter. Any text entered in MQSC in lowercase is converted automatically to uppercase unless you enclose it in single quotation marks. This means that if you create a queue with the name orange.queue, you must refer to it in any commands outside MQSC as ORANGE.QUEUE. The message MQSeries queue created is displayed when the queue is created.

   You have now defined a default queue manager called venus.queue.manager and a queue called ORANGE.QUEUE.
6. To Stop MQSC, press Ctrl-D, or type end and press **Enter**. The following message apears: Enter.

   The following message is displayed:
   - One MQSC commands read. No commands have a syntax error. All valid MQSC commands were processed.

   The command prompt is displayed again.

To test the queue and queue manager, use the samples amqsput (to put a message on the queue) and amqsget (to get the message from the queue) as described in the following steps.

1. Change to /usr/mqm/samp/bin
2. To put a message on the queue, type amqsput ORANGE.QUEUE and press Enter.

   The following message appears:

   ```
   sample amqsput0 start
   ```

   ```
   target queue is ORANGE.QUEUE
   ```
3. Type any message text and press Enter **two times.**

   The following message appears: Sample amqsput0 end

If required, change to /usr/mqm/samp/bin

To get the message from the queue, type `amqsget ORANGE.QUEUE.` and press Enter: The following occurs:

- The sample program starts
- your message is displayed
- the sample ends
- the command prompt is displayed again

The verification is complete.

Installing IBM MQSeries Workflow on AIX

Prerequisites:

1. AIX version 4.3 or higher;
2. IBM WebSphere MQSeries for AIX Version 5.3.0.1 or higheR;
3. IBM DB2 Universal Database for AIX Version 7.2 or higher.

Installing on AIX

Creating user ID and groups

1. Log on as root.
2. Enter command `mkgroup fmcgrp`
3. Verify that MQSeries Administrator **mqm** exists.
4. Verify that DB2 database administrator group **db2iadml** exists.

   If it does not exist, check to see that you have installed DB2 correctly. If your DB2 Administrator group has a different name, be careful to substitute it whenever the default `db2iadml` is mentioned.
5. Follow these steps to create an MQ Workflow Administration user. Note that the MQ Workflow Administration user ID (for example, fmc) must have MQSeries and DB2 administration rights. Use the following command to create the user. The following example assumes the db2 instance is of the db2iadm1 group.

   ```
   mkuser -a pgrp=fmcgrp groups=mqm,db2iadm1 fmc
   ```
6. Set the password for user fmc with the command: passwd `fmc`, Alternatively, you can create the fmc user and the fmcgrp group using SMIT.
7. Modify fmc's login file to include locale information. For example: `export LANG=en_US`. MQSeries Workflow runtime needs that locale information to look up message bundles.
8. Establish the use of db2 environment in fmc's profile. You can achieve this by including in the fmc's profile including the db2profile of the db2 instance which owns the MQSeries Workflow runtime database. For

example, include the following in the fmc's profile. The example assumes the db2inst1 is the instance owner and db2inst1 is used for the MQSeries Workflow runtime database.

```
export DB2INSTANCE=db2inst1
```

```
if [ -e /home/$DB2INSTANCE/sqllib/db2profile ];
then    . /home/$DB2INSTANCE/sqllib/db2profile fi
```

Installing MQSeries Workflow on AIX

The MQSeries Workflow runtime data will use /var/fmc by default. Depend on usage, it would take about 100MB to 400MB of disk space. It is recommended to check to see if the system has sufficient disk space before the installation is attempted.

1. Log in to AIX as root.
2. Insert the MQ Workflow installation disk into the CD-Rom drive.
3. Mount the CD-Rom by entering the command:

   ```
   Mount -oro -v cdrfs /dev/cd0 /cdrom
   ```

   .
4. Copy all the files in the WFInstall directory from the CD-Rom to a temporary directory (for example, /tmp/WFInstall).
5. Specify the locale for this install as well as the following configuration session. For example: export LANG=en_US.
6. Type: CMBWFAIXInstall.sh /cdrom to start installing the MQSeries Workflow. **Tips:** If you choose smitty to install the MQSeries Workflow, do not choose the fmcdefault (default configuration) package. Instead, always follow the next section to prepare the MQSeries Workflow configuration for the EIP workflow.

Configuring MQSeries Workflow in AIX:

1. While still logged on as root, find the CMBWFConfig.AIX.dat file and open it for editing.
2. Update the MQCommunicationAddress entry to replace the localhost with your machine name or IP address. For example:MQCommunicationAddress=hayes.svl.ibm.com
3. If the fmc is not using db2inst1, update the following entries to reflect the proper db2 instance owner.

   RTDB2Instance, RTDB2LocalInstance, RTDatabaseContainerDirectory

   RTDatabaseLocation, RTDatabaseLogLocation
4. The default queue manager for the MQ Workflow is listening to port 5010. Check the /etc/services to see if it is being taken. Update the MQPort entry in the file to a different number if it's needed
5. Save the edited CMBWFConfig.AIX.dat file.

6. Make sure to allow the fmc user to be able to read and run those EIP configuration files as well as write configuration log file into this directory.
7. Make sure there is no errors in the fmc user's .profile as the configuration script will su to fmc.
8. Run the CMBWFAIXConfig.sh under root. You will be prompted to enter fmc's password. This script will create the MQSeries Workflow FMC configuration, create the MQSeries Workflow runtime database FMCDB, create the FMCQM queue manager, create the EIP workflow queue, and define the EIP workflow container data structures.

   Tips: Find the MQSeries Workflow manual references to these MQSeries Workflow utilities: fmczkcfg and fmczutil for usage details on how to customize your MQSeries Workflow configuration. Note that the EIP is default to work with only MQSeries Workflow FMC configuration and FMCQM queue manager. Do not change these settings in your MQSeries Workflow configuration.
9. Type `dspmq`. You should be able to see the FMCQM queue manager registered on the system. For example:

   ```
   QMNAME(FMCQM)                                     STATUS(Ended normally)
   ```
10. Type `fmczkcfg -o=l`. You should be able to see the MQSeries Workflow FMC configuration registered on the system. For example:

   ```
   -  FMC33611I The following configurations are defined: FMC
   ```

   The customization of MQSeries Workflow for the EIP workflow is now completed.

Starting EIP Workflow on AIX: EIP Advanced workflow uses MQSeries Workflow as the underlying workflow engine to deliver workflow functionality. Therefore, starting EIP workflow includes steps to start the MQSeries Workflow.

1. Log on as `fmc`
2. To start the MQSeries Workflow, type: CMBWFAIXStart.sh. You will see console messages being reported while the MQSeries Workflow is starting up.
3. You will be prompted to enter the EIP Administrator user id (i..e, icmadmin) and password in order to start up the EIP collection points monitor.

The EIP collection points monitor will report its startup status via the console. You could modify the line where the CMBWFAIXStart.sh invokes the cmbupes81.sh to give it the user id and password, so you will not be prompted for user id and password next time you run the CMBWFAIXStart.sh script. Type cmbupes81.sh ñh to see possible options

Tip: If you do not require the collection point functionality, enter 'quit' to shutdown the UPES server. Shutting down the UPES server does not shut down the MQSeries Workflow

Tip: You need to enable the WorkFlow Service option in the EIP System Administration client before you could define EIP Workflow objects (such as Workflow processes and actions) via the Administration client. After you enable the Workflow Service in the EIP, it is important to keep in mind to have the MQSeries Workflow running when you log on the System Administration client. This is needed to keep the Workflow objects definitions in sync between the EIP Administration database and the MQSeries Workflow runtime database. Because the EIP System Administration client only runs on the Windows platform, you would need to start the RMI server for the federated connector and the RMI server for the workflow service on the AIX system, and also modify the INI files on the Windows machine to enable the EIP administration client to administer the EIP Administration database on the AIX

Tip: The default MQSeries Workflow system administrator (not configuration administrator) id is ADMIN with default password as ″password″. You would want to change it later for security reason. To do that, first start the MQSeries Workflow and use the fmcautil utility to connect to the Workflow system to change the password. After you have done that, be sure to modify the CMBWFAIXStart.sh to reflect your changes. Here are the steps:

1. `fmcautil ñu admin ñp password`
2. Select `u, p` to change your password and then exit the utility.
3. Update the CMBWFAIXStart.sh. For example:

```
fmcxspea -y=$ConfigurationID -u=$RunTimeAdminID -p=myPassword -f &
```

Chapter 17. Performing pre-installation steps on AIX

In addition to installing all the necessary prerequisites, you need to complete the following tasks before installing Content Manager and Enterprise Information Portal:

- “Confirm the correct version of Java”
- “Create user IDs”
- “Update the .profiles for the new user IDs” on page 237
- “Update the DB2 instance profile.env file” on page 237
- “Create a userprofile file for Content Manager environment settings” on page 237
- “Configure Secure Sockets Layer (SSL) for IBM HTTP server” on page 237
- “Create a staging directory for the resource manager” on page 243
- “Establish the database environment” on page 243

If you had a previous installation of the Content Manager V8 software, be sure to uninstall the product(s) and clean up your environment. Some product files such as configuration files and the databases are purposely left behind after uninstalling. This may affect the success of your installation.

Confirm the correct version of Java

To confirm that you have the correct version of Java, execute the command:

```
# java -version
```

Make sure that the java version 1.3.0 or later is used.

```
java version "1.3.0"
```

Create user IDs

You need to create three user IDs to use with Content Manager and Enterprise Information Portal, as follows:

- Library server ″administration″ user ID (such as `icmadmin`) if you are installing a library server on this workstation. This user ID **must** be part of the DB2 Admin group.
- ″Database connection″ user ID (such as `icmconct`) if you are installing a library server on this workstation. (This should be a regular user ID with normal privileges, not part of the DB2 Admin group.)

- Resource manager ″administration″ user ID (such as `rmadmin`) if you are installing a resource manager on this workstation. This user ID **must** be part of the DB2 Admin group.

The icmadmin user ID and the rmadmin user ID need to be part of the DB2 Admin group. Follow these steps to create each user as part of the db2 administration server group named db2iadm1 (that is, the same group used for your db2 instance):

__ 1. Create the user IDs:

```
# mkuser pgrp=db2iadm1 groups=staff,db2iadm1 icmadmin#
mkuser pgrp=db2iadm1 groups=staff,db2iadm1 rmadmin#
mkuser icmconct
```

__ 2. Assign initial passwords. You can set the initial password value to whatever you want (for example: ″firstone″. The first login will prompt you to change the password).

```
# passwd icmadmin#
passwd rmadmin#
passwd icmconct
```

__ 3. Perform initial login. You are prompted to change the password.

```
# login icmadmin#
login rmadmin#
login icmconct
```

Very important: You need to remember these user IDs and their passwords for entry during the installation. We remind you about them during the installation (at the time that you need to enter them). You can record their names here:

Table 76. Administration and connection IDs

	Default name / information	**Record your value here**
Library server database administration ID	icmadmin	
Library server database administration ID password		
Database connection ID	icmconct	
Database connection ID password		
Resource manager database administration ID	rmadmin	
Resource manager database administration ID password		

Update the .profiles for the new user IDs

Add the following line to /home/icmadmin/ .profile and /home/rmadmin/.profile files:

```
. /home/db2inst1/sqllib/db2profile
```

Note the space between the period (.) and the first slash (/). This will establish the DB2 environment associate the users with the db2inst1 DB2 instance.

Update the DB2 instance profile.env file

If the data is not already in the file, add the following lines to the /home/db2inst1/sqllib/profile.env file:

```
DB2ENVLIST='LIBPATH ICMROOT ICMDLL ICMCOMP EXTSHM CMCOMMON'
DB2COMM='tcpip'
DB2AUTOSTART='TRUE'
```

Create a userprofile file for Content Manager environment settings

Create a file or update the file called:/home/db2inst1/sqllib/userprofile to contain the following data:

```
ICMROOT=/usr/lpp/icm
ICMDLL=/home/db2fenc1
ICMCOMP=/usr/vacpp/bin
CMCOMMON=/usr/lpp/cmb/cmgmt
EXTSHM=ON
PATH=$PATH:$ICMROOT/bin/DB2
LIBPATH=$ICMROOT/lib:$ICMROOT/inso:$LIBPATH
DB2INSTANCE=db2inst1
export ICMROOT ICMDLL ICMCOMP CMCOMMON EXTSHM PATH LIBPATH DB2INSTANCE
```

Do not modify /home/db2inst1/sqllib/db2profile, since this file can be overwritten by the application of a DB2 fixpack. Instead, put any necessary modifications in **userprofile**. When **db2profile** is invoked, it runs **userprofile**. When it runs **userprofile**, it causes all settings added to it to be set for users in **db2profile**. This action establishes the DB2 environment with **db2profile**.

Configure Secure Sockets Layer (SSL) for IBM HTTP server

If you installed WebSphere on this workstation, you need configure Secure Sockets Layer (SSL) for IBM HTTP Server.

This section explains how to configure Secure Sockets Layer (SSL) for IBM HTTP Server on an AIX server to establish secure connections. The resource manager, which requires a web server such as IBM HTTP Server, requires SSL in order to fully communicate with the system administration client. It is important that you follow these instructions very carefully.

Once configured for SSL, you need to enable both http and https access for the resource manager.

See the IBM HTTP Server documentation for the most recent and complete details.

Overview of Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is an encryption system used on servers to ensure that data transferred between a client and a server remains secure and private.

For a server and client to use SSL for secure communications, the server must have two things:

Key pair
A Key pair consists of public and private keys. The keys are used for encryption and decrypting of messages to ensure privacy and confidentiality in transmissions across the internet.

Certificate
The certificates is used for authentication or verification of identity. A certificate can be either self-signed certificate or an issued certificate:

Self-signed
A certificate that you create for your own private Web network

Issued Provided (issued) to you by a *certificate authority* (CA) or by a *certificate signer*.

SSL uses a security handshake to initiate a secure connection between the client and the server. During the handshake, the client and server agree on the keys they will use for the session and the method for encryption. The client authenticates the server using the server certificate.

After the handshake, SSL is used to encrypt and decrypt all of the information in both the HTTPS (a unique protocol that combines SSL and HTTP) request and the server response, including:

- The URL that the client is requesting
- The contents of any form being submitted
- Access authorization information (like user names and passwords)
- All data sent between the client and the server

Configuring secure connections

To have a secure network connection, you will need to complete the following four procedures:

__ 1. Create a new key database (if one does not already exist) and a key.

__ 2. Receive a server certificate from a certificate authority or create a self-signed server certificate using the IBM Key Management Utility (IKEYMAN).

__ 3. Set up SSL using the IBM Administration Server.

__ 4. Test the server installation and configuration.

Creating a new key database

A key database is a file that the server uses to store one or more key pairs and certificates. You can use one key database for all your key pairs and certificates, or create multiple databases. You can create a new key database or you can use an existing key database. If you want to use an existing key database, you can go on to “Creating a self-signed certificate” on page 240.

If you want to create a new key database, continue below.

To create a new key database:

__ 1. Start by creating a directory to store the *keys* database files:

```
# mkdir /usr/HTTPServer/keys
```

This directory must pre-exist when you actually create the files.

__ 2. Enter `ikeyman` on the command line to start the Key Management utility .

__ 3. Click **Key Database File ⟶ New**.

__ 4. In the New window that opens:

a. Enter your key database name in the **File name** field (for example: **key.kdb**)

b. Enter the path to the keys folder (that you created in step 1) in the **Location** field

c. Click **OK**

__ 5. When the Password Prompt window opens:

__ a. Create a password. (A minimum of six characters is required.)

__ b. Confirm the password.

__ c. **Very important:** Select the **Stash the password to a file** check box.

__ d. Click **OK**.

Password Strength guidelines:

You can see the *strength* of the password change by the number of key symbols that appear (up to five keys).You can see five keys appear after you enter a complicated key with mixed-case alpha-numeric characters that include special characters, such as the following example: `MickeyMouse43@#0243`

__ 6. An information window opens to tell you that the password has been encrypted and saved. Click **OK**.

__ 7. Close the IBM Key Management window (**Key Database File → Exit**).

Creating a self-signed certificate

Use `IKEYMAN` to create a self-signed server certificate to enable SSL sessions between clients and the server. Use this procedure if you are acting as your own CA for a private Web network.

__ 1. Enter `ikeyman` on the command line to start the Key Management utility .

__ 2. Click **Key Database File → Open**.

__ 3. In the Open dialog box, navigate to your key database name (for example: C:\keys\key.kdb), then click **Open**.

__ 4. When the Password Prompt window opens, enter your password (that you created in the previous section) and click **OK**.

__ 5. Select **Personal Certificates** from the dropdown list in the **Key Database content** frame, then click the **New Self-Signed...** button.

__ 6. In the Create New Self-Signed Certificate window, you need to know the following information for these fields (the other fields are self explanatory):

Key label
Set your Key label to **icmrm**

Common name
Enter the fully qualified host name of the Web server as the common name (for example: www.myserver.com).

Organization
You need to put some information in this field (for example: the name of your company or organization).

__ 7. When you have completed this panel, click **OK**.

__ 8. You can verify that the new Personal Certificate was created successfully and its name appears in the Personal Certificate panel (for example *icmrm).

__ 9. After creating the self-signed certificate, confirm that all necessary files have been created. In the `/usr/HTTPServer/keys` directory, you should find four files:

```
key.kdb
key.sth
key.crl
key.rdb
```

If you are missing the key.sth file, you forgot to stash the password to a file. Go back and repeat "Creating a new key database" on page 239. Make sure that you check the box to stash the password after you create it.

__ 10. You are now ready to set up SSL using the IBM HTTP administration server.

Close the IBM Key Management window (**Key Database File → Exit**).

Setting up SSL using the IBM HTTP Administration Server

To set up SSL for AIX:

__ 1. Back up the current configuration file /usr/HTTPServer/conf/**httpd.conf**:

```
# cp -p /usr/HTTPServer/conf/httpd.conf
                 /usr/HTTPServer/conf/httpd.conf.save
```

__ 2. Add the following rows into the httpd.conf file as the first item of the Dynamic Shared Object (DSO) Support:

```
 ClearModuleList
AddModule mod_so.c
LoadModule ibm_app_server_http_module
     /usr/WebSphere/AppServer/bin/mod_ibm_app_server_http.so
LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so
```

__ 3. Comment the ClearModuleList line under the stanza of AddModule and under this line add the reference to mod_ibm_ssl.c:

```
 #ClearModuleList
AddModule mod_ibm_ssl.c
....
....
AddModule  mod_setenv_if.c
```

__ 4. Add the port number for the virtual server just below the "Port 80" statement. The default port number for SSL is 443:

```
Port 80
Port 443
```

__ 5. Add the port number for the virtual server just below the "Listen 80" statement. The default port number for SSL is 443:

```
Listen 80
Listen 443
```

__ 6. Check that you have defined the ServerName directive. Change the hostnames in red to the name of your machine, example:

```
ServerName homer.svl.ibm.com
```

__ 7. Add following text-block to the end of the **httpd.conf** (after adjusting hostname in red):

```
<VirtualHost "homer.svl.ibm.com:443 (homer)">
ServerName homer.svl.ibm.com
DocumentRoot /usr/HTTPServer/htdocs/en_US
Keyfile /usr/HTTPServer/keys/key.kdb
SSLV2Timeout 100
SSLV3Timeout 1000
SSLEnable
SSLClientAuth none
SSLServerCert icmrm
SSLCipherSpec 39
SSLCipherSpec 3A
SSLCipherSpec 62
SSLCipherSpec 64
</VirtualHost>
```

__ 8. Save the `httpd.conf` file .

__ 9. Check for the syntax

```
# /usr/HTTPServer/bin/apachectl configtest
```

__ 10. Restart the server.

```
# /usr/HTTPServer/bin/apachectl graceful
```

__ 11. Test the server installation:

__ a. Test the http connection:

From a web browser enter the URL: `http://<hostname>`

__ b. Test the https (SSL) connection:

From a web browser enter the URL: `https://<hostname>`

If SSL is not working, check `/usr/HTTPServer/logs/error_log` for messages. A common error message is ″mod_ibm_ssl: GSK could not initialize, Invalid password for keyfile″. In this case, be sure you choose to stash the password when the key database was created (using the ikeyman utility).

Additional steps for WebSphere Application Server, Version 4 Advanced Edition (AE)

If you have WebSphere Application Server Advanced Edition (AE) installed then the Web Server Plugin needs to be generated with SSL information:

__ 1. Make sure that the WebSphere Application Server (WAS) service is started.

__ 2. Invoke the WebSphere Application Administrative Console.

__ 3. Click **Virtual Hosts** in the tree on the left frame of the console Click the **General** tab on the right frame of the console Click **Add**

__ 4. Enter ***:443** in the text area that appears (that's an asterisk, a **colon**, then the numbers 443).

__ 5. Click **Apply**

__ 6. Click **Nodes** (to expand that part of the tree)

__ 7. Right click <your hostname> in the tree on the left frame

__ 8. Click **Regen Webserver Plugin**

__ 9. Restart the IBM HTTP Server and the WebSphere Application Server so that the latest plugin information takes effect.

Testing the server installation and configuration

After configuring the Secure Sockets Layer, you should test the server installation:

__ 1. Start WebSphere as follows:

for AES

```
/usr/WebSphere/AppServer/bin/startServer.sh
```

for AE

```
/usr/WebSphere/AppServer/bin/startupServer.sh
```

__ 2. Test the http connection:

```
/http://<hostname>/servlet/snoop
```

__ 3. Test the https (SSL) connection:

```
/https://<hostname>/servlet/snoop
```

Create a staging directory for the resource manager

You need to create a staging directory for Content Manager before you begin the installation program. During the installation, you are prompted to provide the staging area directory and its mount point. The installation program assumes you have already created this directory:

```
mkdir /home/ubosstg
```

Establish the database environment

It is **very important** that you establish the DB2 environment. Running db2profile sets the PATH and CLASSPATH and also identifies the DB2 instance that Content Manager will use:

```
. /home/db2inst1/sqllib/db2profile
```

DO NOT forget this step; if you do, Content Manager will not install successfully.

Chapter 18. Installing Content Manager components on AIX

This section is a guide for installing the following Content Manager components on AIX:

- Library server
- Resource manager
- The Information center

Information for installing the other client components are covered in the following sections:

- Chapter 15, “Installing the Content Manager Client for Windows”, on page 205
- Chapter 22, “Installing the Content Manager eClient on AIX”, on page 319

Before you begin

Before you begin the Content Manager installation:

__ 1. There are special instructions provided for the following required program products:

IBM DB2 Universal Database or Oracle database

An IBM DB2 Universal Database or an Oracle database is required for the library server and the resource manager.

If you have not already installed your database application:

- See “IBM DB2 Universal Database” on page 217 for instructions for installing your DB2 database on the workstation.

  The database must be installed on your workstation **before** you begin the installation of the Content Manager components.
- See “Oracle database on a Solaris system” on page 335 for instructions for installing your Oracle database on the workstation.

  If the library server application and the library server database will be installed on separate machines:

  a. The library server database **must be created before** the library server application component can be installed.

  b. The library server database on the remote Oracle server must be up and running and have an active Oracle listener associated with it. DB2 will connect to the Oracle database during the library server application installation using the tnsnames and Net8 protocol.

IBM DB2 Universal Database client software
For Oracle/resource manager installations, IBM DB2 client software is required to be installed. (The DB2 JDBC drivers are needed for communication of the resource manager with the library server.)

DB2 Text Information Extender (TIE)
Text Information Extender (TIE) or Net Search Extender (NSE) is required if you plan to use the Text Search feature.

See "IBM DB2 Net Search Extender (NSE) and Text Information Extender (TIE)" on page 227 for instructions for installing Text Information Extender (TIE) or Net Search Extender (NSE).

NSE or TIE must be installed on the same workstation as the library server.

IBM WebSphere Application Server (WAS)
IBM WebSphere Application Server is required for the resource manager.

See "IBM WebSphere Application Server (WAS)" on page 228 for instructions for installing and configuring WAS on the workstation. 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.

Tivoli Storage Manager
Chapter 30, "Installing and Configuring Tivoli Storage Manager (TSM)", on page 431 provides the instructions for installing and configuring TSM. TSM is an optional feature that provides long-term storage on devices other than the fixed disks attached to the resource manager. It is installed after the resource manager component is installed.

__ 2. Ensure that your system meets all of the memory, hardware, and all other software requirements to install Content Manager. Refer to "AIX requirements" on page 59 for a summary of these requirements.

__ 3. Make sure that the following products that are shipped with AIX are installed on your machine:
- TCP/IP
- AIX windows
- Unicode converter (bos.iconv.ucs.pc), which includes:
  – Common Language to Language Converters
  – Unicode Converters for AIX Code Sets
  – Unicode Converters for Additional PC Code Sets

- Unicode Converters for EBCDIC Code Sets

__ 4. Make sure that the locale the install program runs under is the same as the one the administration IDs of the selected components have. Otherwise, during runtime, the correct message files and language dependent files may not be available. For example, when you start the AIX install program, the LANG environment variable is set to ″En_US″, but the locale for the Library Server Administration ID is set to ″en_US″. In this case, only the message files of ″En_US″ locale are installed. Consequently, when you start the Library Server, you will get error message indicating that the message cannot be resolved. This is a minor problem for the English locale but could be a problem to locales such as Italian, Japanese, and others when the regional character set is different between ″it_IT″ and ″IT_IT″, for example.

Installing Content Manager on AIX

To start the installation, complete the following steps:

__ 1. Verify that you have created the three necessary user IDs that are needed for the installation:

- Library server ″administration″ user ID (such as `icmadmin`) if you are installing a library server on this workstation. This user ID **must** be part of the DB2 Admin group.
- ″Database connection″ user ID (such as `icmconct`) if you are installing a library server on this workstation. (This should be a regular user ID with normal privleges, not part of the DB2 Admin group.)
- Resource manager ″administration″ user ID (such as `rmadmin`) if you are installing a resource manager on this workstation. This user ID **must** be part of the DB2 Admin group.

If you do not have the three user IDs, see “Create user IDs” on page 235 for detailed instructions for creating them.

__ 2. Modify .profile of `icmadmin` and of `rmadmin` to include the following lines:

```
ICMROOT=/usr/lpp/icm

ICMDLL=/home/<db2fenc1>

ICMCOMP=/usr/vacpp/bin

CMCOMMON=/usr/lpp/cmb/cmgmt

EXTSHM=ON

PATH=$PATH:$ICMROOT/bin/DB2

LIBPATH=$ICMROOT/lib:$LIBPATH

DB2INSTANCE=<DB2_INSTANCE_NAME>

DB2LIBPATH=$ICMROOT/lib:$DB2LIBPATH
```

```
export ICMROOT ICMDLL ICMCOMP CMCOMMON ESTSHM PATH LIBPATH
       DB2INSTANCE DB2LIBPATH
```

Where:

ICMROOT is the Content Manager product install location

ICMDLL is the DB2 fence location (This is set to home of DB2fence because the fenceID creates the DLL dynamically at run time)

ICMCOMP is the VisualAge C++ compiler location

CMCOMMON is the shared area for Content Manager and Enterprise Information Portal configuration files

EXTSHM is for use shared memory

__ 3. Add these lines to .profile of `icmadmin` and of `rmadmin` (if they are not already there)

```
if [[ -e /home/$DB2INSTANCE/sqllib/db2profile ]] then;
. /home/$DB2INSTANCE/sqllib/db2profile
fi
```

__ 4. Modify `/home/<$DB2INSTANCE>/sqllib/profile.env to have the following lines` (if `profile.env` does not exist, create it):

```
DB2ENVLIST='LIBPATH ICMROOT ICMDLL ICMCOMP EXTSHM CMCOMMON
DB2LIBPATH'
```

```
DB2COMM='tcpip'
```

__ 5. Shut down any DB2 applications, then stop and start DB2 with one of the following procedures:

- If you are installing a library server on this machine, login as a the library server admininistrator (for example: icmadmin) to shut down any open DB2 applications, then stop and start DB2 with the same user ID.
- If you are only installing a resource manager on this machine, login as a the resource manager admininistrator (for example: rmadmin) to shut down any open DB2 applications, then stop and start DB2 with the same user ID.
- If you are installing both a library server and a resource manager, and if they are being installed against separate DB2 instances, you need to shut down DB2 applications, then stop and start DB2 using both administrator IDs (for example: icmadmin and rmadmin).

Important

a. Whenever you start Content Manager, start it with the library server user ID (<icmadmin>) or the resource manager user ID (<rmadmin>) to ensure that the Content Manager applications can reference required environment variables, which are exported through the profiles of those administrators.

b. Whenever you start WebSphere Application Server for the resource manager, make sure that you have the following environment variable set as follows:

```
EXTSHM=ON
```

__ 6. **For Oracle only:** Make the library server user ID that was created during the installation of DB2 a member of the same group as the Oracle user ID. (For example: make the user ID ICMADMIN a part of the *oinstall* group).

__ 7. **For Oracle only:** Grant **Write permission** for the group in the previous step (for example: *oinstall*) to the `tnsnames.ora` file, located in the directory specified by the Oracle environment variable `TNS_ADMIN`. During the Content Manager installation process, you will be prompted for the value of `TNS_ADMIN`. This value must be consistent with the Oracle installation that you intend for use with Content Manager.

__ 8. **For Oracle only:** Verify that the library server database is up and running by logging on to your Oracle client machine:

```
tnsping LS db name.Oracle server domain name
```

If the connection is successful, proceed with the library server application installation. If the connection is not successful, correct the TNS errors reported by Oracle before continuing:

a. Check the `tnsnames.ora`, `listener.ora`, and `sqlnet.ora` files on your Oracle machine for proper configuration.

b. Recycle the Oracle listener on your Oracle server (if necessary) by performing the following steps:

```
lsnrctl stop
lsnrctl start
```

c. Issue the following command to your Oracle server to ensure that your library server database is associated with the active listener:

```
lsnrctl status
```

__ 9. **For Oracle only:** If you experience connectivity problems , for each HOST in the DESCRIPTION section of the tnsnames.ora file, you might need to update the hosts file:

```
/etc/hosts
```

Whether you update this file or not depends on how TCP/IP is configured on your network. Part of the network must translate the remote host name specified in the DESCRIPTION section in the tnsnames.ora file to an address. If your network has a named server that recognizes the host name, you do not need to update the TCP/IP hosts file. Otherwise, you need an entry for the remote host. See your network administrator to determine how your network is configured.

__ 10. Stop the IBM HTTP Server service.

__ 11. Insert the CD-ROM into your CD-ROM drive.

__ 12. Log in as root (or as a user with root authority)

__ 13. Make sure that your Java JRE Version 1.3 is in the PATH, for example:

```
/usr/java130/sh:/usr/java130/jre/sh:$PATH
```

__ 14. Mount your Content Manager CD-ROM, for example:

```
mount -rv cdrfs /dev/cd0 /cdrom
```

__ 15. Change to the directory where the CD-ROM is mounted by entering the cd /cdrom command, where cdrom is the mount point of your Content Manager installation CD-ROM.

__ 16. As root, execute the following command to to get db2 into PATH.CLASSPATH:

```
. /home/$DB2INSTANCE/sqllib/db2profile
```

__ 17. Start the installation wizard by entering the following:

```
setup.exe
```

Welcome panel

The first panel (Welcome) of the InstallShield Wizard opens.

Click **Next**.

Software License Agreement panel

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

Click **Next** to continue the installation.

Step 1. Selecting the components to install

The Component Selection window opens, showing you what components are available to install.

Select the components that you want to install. (By default, all components are checked.)

- Click in the box to remove the check mark of the components that you do not want to install.
- Leave a check mark in the box for each component that you want to install.

Click **Next** when you are satisfied with your selections.

Depending on the selections that you made on this panel, go to the page indicated in Table 77.

Table 77. Location of next step

Choices	Go to
Library server with IBM DB2 (either alone or with any, or all, of the other components)	"Step LS1. Configure Library Server"
Library server with Oracle (either alone or with any, or all, of the other components)	"Step ORA1. Select Library Server Components" on page 259
Resource manager with IBM DB2 only (no other components selected)	"Step RM1. Configure Resource Manager Server" on page 253
Resource manager with Oracle only (no other components selected)	"Step ORA2. Select Resource Manager Components" on page 260
Resource manager with IBM DB2 and Information center	"Step RM1. Configure Resource Manager Server" on page 253
Resource manager with Oracle and Information center	"Step ORA2. Select Resource Manager Components" on page 260
Information center only	"Step VE1. Verify the install location" on page 276

Step LS1. Configure Library Server

Skip this step if you are not installing the library server component at this time, and continue with "Step RM1. Configure Resource Manager Server" on page 253.

Enter the following information for your library server database:

Table 78. Library server configuration

Install information	Description	Default name / option	Record your value here
Library server database name	The name of the library server database	ICMNLSDB	

Table 78. Library server configuration (continued)

<table>
<tr><th>Install information</th><th>Description</th><th>Default name / option</th><th>Record your value here</th></tr>
<tr><td>Library server schema name</td><td>The library server schema name</td><td>ICMADMIN</td><td></td></tr>
<tr><td>Library server database administration ID</td><td>Administration ID for the library server[1]</td><td>icmadmin</td><td></td></tr>
<tr><td>Password</td><td>Password for the library server administration ID[1]</td><td>&lt;password&gt;</td><td></td></tr>
<tr><td>Database connection ID</td><td>Database connection ID [2]</td><td>icmconct</td><td></td></tr>
<tr><td colspan="4"><b>Note:</b>
1. This is the administration ID that you created at the beginning of the install process. See Table 76 on page 236.
2. This is the database connection ID that you created at the beginning of the install process. See Table 76 on page 236.</td></tr>
</table>

When you complete your library server configuration, click **Next**.

Program note:

1. At this time the installation program checks to see if a Content Manager (CM) library server database or an Enterprise Information Portal (EIP) system administration database exist on this workstation.

   If a database exists, the program checks to see if it has the same database name, the same user ID, the same schema name, or the same password that you entered.

   - If (only) a CM library server database already exists, the program asks if you want to overwrite the existing database, keep it, or go back to type in new information for the new database.
   - If (only) an EIP system administration database exists, the program asks if you want to share the database between CM and EIP, or if you want to type in another name for the new CM library server database. The installation program cannot create a new separate library server database with the same name as the system administration database. You must give it a different name than the system administration database.

- If a shared database between CM and EIP already exists, the program asks if you want to proceed with no change to the existing database, or to go back and enter a new information for the database that you want to create.

2. Also, during the time that the library server is being installed, a program called ″library server monitor″ is being created automatically. The library server monitor program's job is to detect the availability of resource managers to a library server database (among other things that are listed in the section called "Running the library server monitor program" on page 498.).

   If the library server monitor program ever stops running abnormally, then you need to restart it by using the procedure that is also described in the section called "Running the library server monitor program" on page 498.

Step LS2. Configure Library Server Options

Select the library server options:

Table 79. Library server configuration options

Install information	Description	Default name / option	Record your value here
Name of library server ID	Enter the name of the library server ID (Range = 1 to 99)	1	
Enable Unicode (check box)	Check this box to enable Unicode .	(not checked)	
Enable text search (check box)	Check this box if you want to use the Text Search feature. [1]	(not checked)	

Note:

1. You must have the DB2 Text Information Extender (TIE) or DB2 Net Search Extender (NSE) installed to use Text Search.

Click **Next** to continue to the next window.

Step RM1. Configure Resource Manager Server

Skip this step if you are not installing the resource manager component at this time, and continue with "Step CNLS1. Connect Library Server To Resource Manager" on page 256

Enter the identification and authentication information for the resource manager:

Table 80. Configuring the resource manager server

Install information	**Description**	**Default name / option**	**Record your value here**
Resource manager database name	The name of the resource manager database	RMDB	
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>	
Note: 1. This is the Administration ID that you created at the beginning of the install process. See Table 76 on page 236.			

When you complete your resource manager configuration, click **Next**.

Program 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.

Step RM2. Configure Resource Manager Server Options

Enter the information for the resource manager mount point, and staging area path:

Table 81. Resource manager server options

Install information	**Description**	**Default name / option**	**Record your value here**
Mount point	Location of the storage area that is used for storing objects	/home[1]	
Staging area path	Location of the storage area that is used for staging LAN Cache objects or TSM objects	/home/ubosstg/	

Table 81. Resource manager server options (continued)

Install information	Description	Default name / option	Record your value here
Note: 1. This is where resource manager objects are stored. Ensure that you have sufficient space on this file system.			

Click **Next** to continue to the next window.

Step RM3. Deploy Resource Manager With WebSphere Application Server

Enter the following information to identify the application server that your resource manager will use:

Table 82. Deploying the resource manager

Install information	Description	Default name / option	Record your value here
WAS home	Location of the WebSphere Application Server program[1]	/usr/WebSphere /AppServer	
Web application path	The web path to the WebSphere application server	/icmrm	
Web application name	The name of the Web application	icmrm	
Services port	Enter a port number (the first of five numbers) to be used for resource manager components (migrator, purger, stager, replicator, and asynchronous recovery)	<recommendPort> The recommended port number is displayed on the panel[2].	
Node name	Enter the node name for this resource manager application	<current machine node name>	
WAS administrator user name	Enter the WAS administrator user ID	was_admin	

Table 82. Deploying the resource manager (continued)

Install information	Description	Default name / option	Record your value here
Password (two fields)	Enter and confirm the password for the WAS Admin user name	<password>	
Application server name [3]	The name of the WAS AE application server[3]	ICMRM	
Note: 1. The installation program deploys icmrm.war only if WebSphere Version 4.0.3 (or later) is installed on this workstation. (See the README for the latest information.) 2. You can enter a port number other than the recommended default number. However, it must be the first number of five available contiguous port numbers. 3. **Special use field:** This field is only used if WebSphere Application Server Advanced Edition (AE) is installed on this workstation.			

Click **Next** to continue to the next window.

Step CNLS1. Connect Library Server To Resource Manager

Skip this step if any one of the conditions listed in Table 83 are true, and continue with the step indicated. Otherwise, continue below.

Table 83. Location of next step

Condition	Continue with (go to)
If you are not installing a library server or a resource manager at this time	"Step VE1. Verify the install location" on page 276
If you are installing a resource manager, **but not** a library server at this time	"Step CNRM. Connect Resource Manager To Library Server" on page 258

Enter the information about the resource manager that the library server needs to connect to it:

Table 84. Connect library server to resource manager

Install information	Description	Default name / option	Record your value here
Resource manager server host name	The fully qualified host name of the workstation that contains the resource manager	<hostName>	
Resource manager database name	The name of the resource manager database	RMDB	
Web application port number	The port number for the Web Application Server	80	
Secure Web application port (HTTPS)	Port number for the resource manager to communicate with the system administration client	443	
Web application path	Same as the path entered in "Step RM3. Deploy Resource Manager With WebSphere Application Server" on page 255	/icmrm	
Resource manager server operating system (drop-down list of available choices)	The operating system of the workstation where the resource manager is located	<platform>	
Token duration (hours)	The amount of time (in hours) that a connection between the library server and the resource manager can stay active until it is discarded by the system. (Can be modified later with the system administration client tools.)	48	

Click **Next** to continue to the next window.

Step CNLS2. Connect Library Server To Resource Manager Part 2

Skip this step if the library server and the resource manager are being installed on the same machine.

Enter the resource manager database connection ID and password:

Table 85. Resource manager connection ID

Install information	Description	Default name / option	Record your value here
Resource manager database administration ID	See Note 1 (below).	rmadmin	
Password	See Note 1 (below).	<password>	
Note: 1. These are the same values that were entered during "Step RM1. Configure Resource Manager Server" on page 253.			

Click **Next** to continue to the next window.

Step CNRM. Connect Resource Manager To Library Server

Skip this step if you are not installing a resource manager at this time, or if the library server and the resource manager are being installed on the same machine.

Enter the information about the library server that the resource manager needs to connect to it:

Table 86. Connect resource manager to library server

Install information	Description	Default name / option	Record your value here
Library server host name	The host name of the workstation that contains the library server	<host name>	
Library server database name	See Note 1 (below).	ICMNLSDB	
Library server schema name	See Note 1 (below).	ICMADMIN	

Table 86. Connect resource manager to library server (continued)

Install information	Description	Default name / option	Record your value here
Library server database administration ID	See Note 1 (below).	icmadmin	
Password	See Note 1 (below).	<password>	

Note:

1. These are the same values that were entered during “Step LS1. Configure Library Server” on page 251.

Click **Next** to continue with “Step LDAP1. Configure Components for LDAP” on page 273.

Step ORA1. Select Library Server Components

Skip this step if you are not installing a library server (with Oracle) on this machine.

Select the library server components to install on this machine, and enter the location of the configuration file:

Table 87. Select library server components

Install information	Description	Default name / option	Record your value here
Library server database	Check this box to install the library server database on this machine	(checked)	
Library server application	Check this box to install the library server application on this machine	(checked)	
Location of the default configuration settings file	Path to the default configuration settings file[1]	Default	

Notes:

1. For more information about this field, see “Oracle - expanded information for installation panel fields” on page 276.

Click **Next** to continue to the next window.

Step ORA2. Select Resource Manager Components

Skip this step if you are not installing a resource manager (with Oracle) on this machine.

Select the resource manager components to install on this machine, and enter the location of the configuration file:

Table 88. Select resource manager components

Install information	Description	Default name / option	Record your value here
Library server database	Check this box to install the resource manager database on this machine	(checked)	
Library server application	Check this box to install the resource manager application on this machine	(checked)	
Location of the default configuration settings file	Path to the default configuration settings file[1]	Default	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.

Click **Next** to continue to the next window.

Step ORA3. Configure Oracle Database (1)

Enter the information for the Oracle database server:

Table 89. Oracle server database

Install information	Description	Default name / option	Record your value here
Base directory for Oracle	This is the fully-qualified path under which all Oracle products can be found.[1]	/Oracle	

Table 89. Oracle server database (continued)

Install information	Description	Default name / option	Record your value here
Oracle database server directory	This is the fully-qualified path to your Oracle Enterprise Edition product directory. [1]	/Oracle/Ora92	
Oracle TNS Names file location	This is the fully-qualified path to the `tnsnames.ora` file in use for the ORACLE_HOME environment variable.[1]	/Oracle/Ora92/ network\admin	
Oracle NLS message files location	This is equivalent to your ORA_NLS33 environment variable.[1]	/Oracle/Ora92/ ocommon/nls/ admin/data	
Oracle JDBC path	Click **Browse** to find the path to the JDBC directory		
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.			

Click **Next** to continue to the next window.

Step ORA4. Configure Oracle Database (2)

Enter information for the Oracle database server:

Table 90. Oracle database

Install information	Description	Default name / option	Record your value here
Oracle database server version	Select the version of the installed Oracle software[1]	9.2.0.1 OR higher	
Password (two fields)	Enter and confirm the password for the Oracle SYSTEM and SYS user IDs[1]	<password>	

Table 90. Oracle database (continued)

Install information	Description	Default name / option	Record your value here
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.			

Click **Next** to continue and go to the first step indicated by the following questions:

1. Are you installing a library server database or a library server application on this machine?

   If **yes**, go to question 2.

   If **no**, go to question 3.
2. Are you installing a library server application on this machine?

   If **yes**, go to "Step OLS1. Configure Library Server Application (1)".

   If **no**, go to "Step OLS6. Configure Library Server Database (1)" on page 266.
3. Are you installing a resource manager database on this machine?

   If **yes**, go to "Step ORM1. Configure Resource Manager Database (1)" on page 268.

   If **no**, go to "Step ORM5. Configure Resource Manager Application (1)" on page 271.

Step OLS1. Configure Library Server Application (1)

Skip this step if you are not installing a library server application on this machine, and go to "Step OLS6. Configure Library Server Database (1)" on page 266.

Enter the information for the library server application to connect to the library server database:

Table 91. Configure library server connections

Install information	Description	Default name / option	Record your value here
Library server database name	Enter the library server database name	ICMNLSDB	
Library server schema name	Enter the library server schema name	ICMADMIN	

Table 91. Configure library server connections (continued)

Install information	Description	Default name / option	Record your value here
Library server database administration ID	This is the user ID that is used to administer your Content Manager library server[1]	oraadmin	
Password (two fields)	Enter and confirm the password	<password>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.			

Click **Next** to continue to the next window.

Step OLS2. Configure Library Server Application (2)

Enter the information for library server database connection ID:

Table 92. Library server connection ID

Install information	Description	Default name / option	Record your value here
Library server database connection ID	Enter the library server database connection ID	ICMCONCT	
DB2 instance owner ID	This is the ID that you created prior to installing the DB2 product.[1]	DB2INST1	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.			

Click **Next** to continue to the next window.

Step OLS3. Configure Library Server Application (3)

Enter the information for library server application options:

Table 93. Library server application options

Install information	Description	Default name / option	Record your value here
DB2 database location	Fully qualified path to the location of the DB2 database that is used with this Oracle database		
Enable unicode	Select to enable unicode	(not checked)	

Click **Next** to continue to the next window.

Step OLS4. Configure Library Server Application (4)

Enter the information for connecting the library server application to the resource manager server:

Table 94. Library server application connection to resource manager

Install information	Description	Default name / option	Record your value here
Resource manager server host name	Enter the resource manager server host name	<hostname>	
Resource manager database administration ID	Enter the resource manager database administration ID	RMADMIN	
Password (two fields)	Enter and confirm the password for the resource manager database administration ID	<password>	

Click **Next** to continue to the next window.

Step OLS5. Configure Library Server Application (5)

Enter more information in this window for connecting the library server application to the resource manager server:

Table 95. Library server application connection to resource manager

Install information	Description	Default name / option	Record your value here
Web application name	Enter the web application name	icmrm	
Web application path	Enter the path for the web application	/icmrm	
Web application port	Enter the port number for the web application	80	
Secure web application port (HTTPS)	Enter the port number for the secure web application	443	
Token duration (hours)	The amount of time (in hours) that a connection between the library server application and the resource manager can stay active until it is discarded by the system. (Can be modified later with the system administration client tools.)	20	

Click **Next** to continue and go to the first step indicated by the following questions:

1. Are you installing a library server database on this machine?

   If **yes**, go to "Step OLS6. Configure Library Server Database (1)" on page 266.

   If **no**, go to question 2.

2. Are you installing a resource manager database or a resource manager application on this machine?

   If **yes**, go to question 3.

   If **no**, go to "Step LDAP1. Configure Components for LDAP" on page 273.

3. Are you installing a resource manager database on this machine?

   If **yes**, go to "Step ORM1. Configure Resource Manager Database (1)" on page 268.

If **no**, go to “Step ORM5. Configure Resource Manager Application (1)” on page 271.

Step OLS6. Configure Library Server Database (1)

Skip this step if you are not installing a library server database on this machine and go to “Step ORM1. Configure Resource Manager Database (1)” on page 268.

Enter information for the library server database:

Table 96. Library server database

Install information	Description	Default name / option	Record your value here
Library server database name	Enter the library server database name	ICMNLSDB	
Library server database location	Enter the fully-qualified path name of the location where you want Oracle to store its internal database files.[1]		
Library server host name	This is the host-only name of the Oracle server where your library server database is created.[1]	<hostname>	
Library server domain name	This is the domain name that is associated with the host name for the library server (in the row above this one).	<xmpl.name.com>	
Notes: 1. For more information about this field, see “Oracle - expanded information for installation panel fields” on page 276.			

Click **Next** to continue to the next window.

Step OLS7. Configure Library Server Database (2)

Enter more information for the library server:

Table 97. Library server database (more information)

Install information	Description	Default name / option	Record your value here
Oracle listener name	Enter the name of the Oracle listener[1]	LISTENER	
Oracle protocol	Select the protocol from the drop-down list[1]	TCP/IP	
Oracle listener port	Enter the port number for the Oracle listener[1]	1521	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.			

Click **Next** to continue to the next window.

Step OLS8. Configure Library Server Database (3)

Enter the authentication information for the library server database:

Table 98. Oracle database administration ID

Install information	Description	Default name / option	Record your value here
Oracle database administration ID	Enter the Oracle database administration ID[1]	oraadmin	
Password (two fields)	Enter and confirm the password for the Oracle database administration ID[1]	<password>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.			

Click **Next** to continue to the next window.

Step OLS9. Configure Library Server Database (4)

Select the configuration options for the library server database:

Table 99. Library server database configuration options

Install information	Description	Default name / option	Record your value here
Enable for unicode	Check this box to enable for unicode	(not checked)	
Mirror database files	Check this box to mirror database files	(checked)	
Mirror directory	Enter (or browse to) the path for the Mirror directory[1]		

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.

Click **Next** to continue and go to the first step indicated by the following questions:

1. Are you installing a resource manager database or a resource manager application on this machine?

   If **yes**, go to question 2.

   If **no**, go to "Step LDAP1. Configure Components for LDAP" on page 273.

2. Are you installing a resource manager database on this machine?

   If **yes**, go to "Step ORM1. Configure Resource Manager Database (1)".

   If **no**, go to "Step ORM5. Configure Resource Manager Application (1)" on page 271.

Step ORM1. Configure Resource Manager Database (1)

Skip this step if you are not installing a resource manager database on this machine, and go to "Step ORM5. Configure Resource Manager Application (1)" on page 271.

Enter information for the resource manager database:

Table 100. Resource manager database

Install information	Description	Default name / option	Record your value here
Resource manager database name	Enter the resource manager database name	RMDB	
Resource manager database location	Enter the fully-qualified path name of the location where you want Oracle to store its internal database files.[1]		
Resource manager host name	This is the host-only name of the Oracle server where your resource manager database is created.[1]	<hostname>	
Resource manager server domain name	This is the domain name that is associated with the host name for the resource manager (in the row above this one).	<xmpl.name.com>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.			

Click **Next** to continue to the next window.

Step ORM2. Configure Resource Manager Database (2)

Enter more information for the resource manager:

Table 101. Resource manager database (more information)

Install information	Description	Default name / option	Record your value here
Oracle listener name	Enter the name of the Oracle listener[1]	LISTENER	

Table 101. Resource manager database (more information) (continued)

Install information	Description	Default name / option	Record your value here
Oracle protocol	Select the protocol from the drop-down list[1]	TCP/IP	
Oracle listener port	Enter the port number for the Oracle listener[1]	1521	
Notes: 1. For more information about this field, see “Oracle - expanded information for installation panel fields” on page 276.			

Click **Next** to continue to the next window.

Step ORM3. Configure Resource Manager Database (3)

Enter the authentication information for the resource manager database:

Table 102. Oracle database administration ID

Install information	Description	Default name / option	Record your value here
Oracle database administration ID	Enter the Oracle database administration ID[1]	RMADMIN	
Password (two fields)	Enter and confirm the password for the Oracle database administration ID[1]	<password>	
Notes: 1. For more information about this field, see “Oracle - expanded information for installation panel fields” on page 276.			

Click **Next** to continue to the next window.

Step ORM4. Configure Resource Manager Database (4)

Select the configuration options for the resource manager database:

Table 103. Resource manager database configuration options

Install information	Description	Default name / option	Record your value here
Mirror database files	Check this box to mirror database files	(checked)	
Mirror directory	Enter (or browse to) the path for the Mirror directory[1]		

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 276.

Click **Next** to continue to the next window.

Step ORM5. Configure Resource Manager Application (1)

Skip this step if you are not installing a resource manager application on this machine, and go to "Step LDAP1. Configure Components for LDAP" on page 273.

Enter information for the resource manager application:

Table 104. Resource manager application

Install information	Description	Default name / option	Record your value here
Web application server name	Enter the web application server name	icmrm	
Web application name	Enter the web application name	icmrm	
Web application path	Enter (or browse to) the path for the web application	/icmrm	
Node name	Enter the node name for this resource manager application	<current machine node name>	
WAS administrator user name	Enter the WAS administrator user ID	was_admin	

Table 104. Resource manager application (continued)

Install information	Description	Default name / option	Record your value here
Password (two fields)	Enter and confirm the password for the WAS Admin user name	<password>	

Click **Next** to continue to the next window.

Step ORM6. Configure Resource Manager Application (2)

Enter information for the resource manager appliction:

Table 105. Resource manager application mount point and staging area

Install information	Description	Default name / option	Record your value here
Mount point	Enter the location of the storage area that is used for storing objects		
Staging area path	Enter the location of the storage area that is used for staging LAN Cache objects or TSM objects		
Resource manager services port	Enter a port number (the first of five numbers) to be used for resource manager components (migrator, purger, stager, replicator, and asynchronous recovery)	<recommendPort> The recommended port number is displayed on the panel[1].	
Note: 1. You can enter a port number other than the recommended default number. However, it must be the first number of five available contiguous prot numbers.			

Click **Next** to continue to the next window.

Step ORM7. Configure Resource Manager Application (3)

Enter information for the resource manager to connect to the library server:

Table 106. Connect the resource manager to the library server

Install information	Description	Default name / option	Record your value here
Library server host name	Enter the library server host name	<hostname>	
Library server database name	Enter the library server database name	ICMNLSDB	
Library server schema name	Enter the library server schema name	ICMADMIN	

Click **Next** to continue to the next window.

Step ORM8. Configure Resource Manager Application (4)

Enter additional information for the resource manager to connect to the library server:

Table 107. Library server application administration ID

Install information	Description	Default name / option	Record your value here
Library server application administration ID	Enter the library server application administration ID	oraadmin	
Password (two fields)	Enter and confirm the password for the library server application administration ID	<password>	

Click **Next** to continue to the next window.

Step LDAP1. Configure Components for LDAP

On this panel, you decide if you want to enable LDAP (Lightweight Directory Access Protocol).

Select the components that you want to enable for LDAP:

Table 108. Enable LDAP options

Install information	Description	Default name / option	Record your value here
Library server (check box)	Check this box to allow user authentication for the library server by an LDAP server	(not checked/No)	
Resource manager server (check box)	Check this box to allow user authentication for the resource manager by an LDAP server	(not checked/No)	
Note: 1. If you enabled (or plan to enable) LDAP for your the system administration client (during its installation), it is a good idea to also check the library server check box (to allow user authentication for the library server)			

Click **Next** to continue.

Step LDAP2. Define LDAP Server

Skip this step if you did not select to Enable LDAP for any components in the previous step, and continue with "Step VE1. Verify the install location" on page 276.

Enter the information for the LDAP server that you want to use:

Table 109. Define the LDAP server

Install information	Description	Default name / option	Record your value here
LDAP server type (drop-down list of available choices)	Select either **Standard LDAP**[1] or **Active Directory**	Standard LDAP	
Host name	Enter the host name of the LDAP server machine	ldap://ldapServer.ibm.com	

Table 109. Define the LDAP server (continued)

Install information	Description	Default name / option	Record your value here
Port	Enter the port number on the LDAP server machine	389	
LDAP server administration ID	Enter the LDAP server administration ID for LDAP on the LDAP server machine	cn = root (default for IBM Directory) <adminId> (default for Active Directory)	
Password	Enter the password for the LDAP server administration ID	<password>	
Note: 1. Select Standard LDAP for IBM Directory or for Domino NAB.			

Click **Next** to continue to the next window.

Step LDAP3. Configure LDAP Server

Enter configuration information for the LDAP server

Table 110. Configure the LDAP server

Install information	Description	Default name / option	Record your value here
Base distinguished name	Refer to the LDAP documentation for information about the base distinguished name	o=ibm, c=US	
User authentification attribute	Refer to the LDAP documentation for information about the user authentification attribute	cn	
Search scope	During search operations against an LDAP, search at one level or in a subtree fashion[1]	Subtree	

Table 110. Configure the LDAP server (continued)

Install information	Description	Default name / option	Record your value here
Referral	Choose to **Ignore** or **Follow** a reference to another LDAP server[1]	Ignore	
Note: 1. See the LDAP documentation for more information			

Click **Next** to continue to the next window.

Step VE1. Verify the install location

Verify that the installation information is correct. If any information is incorrect, you can return to previous windows by using the **Back** buttons. Click **Next** to complete the installation.

The Content Manager install program goes to work

The Start Copying Files window opens.

You will see a message that installation has been successful. Click **Finish**.

You can view the installation logs at the following location:

```
/usr/lpp/icm/logs
```

Verify the installation

After the installation is complete, you can go to the Windows workstation that has the system administration client installed to verify that the installation is successfull. See "First steps - verify the installation" on page 147.

Oracle - expanded information for installation panel fields

This section is provided to give more detail for the information that is added to specific fields during the installation.

Location of the default configuration settings file

You can re-use an existing `icmlsdb.properties` for the library server (or `icmrmdb.properties` file for the resource manager) file as input to the installation process. If no path is provided, values from a default version of the file will be used by install. You can modify or accept these values during the course of the installation. It is also possible to have a custom-made `icmlsdb.properties` file for the library server (or `icmrmdb.properties` file for the resource manager) for use in deploying a new library server (or Resource Manager). However, this is not recommended due to the importance of the accuracy of the information in the icmlsdb.properties for the library server (or icmrmdb.properties file for the resource manager) file.

Base directory for Oracle

This is the fully-qualified path under which all Oracle products can be found. During your initial installation of the Oracle product, you were asked for this value during Oracle product installation. This is the ORACLE_BASE environment variable. For example, if you have installed both Oracle Enterprise Edition and the Oracle Universal Installer, you might have a directory tree similar to the following:

```
/opt/oracle/  ---> /opt/oracle/product/8.1.7
                  |
                   --> /opt/oracle/oui
```

In this example, /opt/oracle would be the value of your ORACLE_BASE environment variable.

Oracle database server directory

This is the fully-qualified path to your Oracle Enterprise Edition product directory. Under this directory is the Oracle database bin, network, dbs, and other related directories. This is equivalent to your ORACLE_HOME environment variable. In the example above, the ORACLE_HOME value would be /opt/oracle/product/8.1.7

Oracle TNS Names file location

This is the fully-qualified path to the tnsnames.ora file in use for the ORACLE_HOME environment variable that you specified in the previous step. The value for this field is equivalent to your Oracle TNS_ADMIN environment variable. The oracle user ID should have full access to this TNS_ADMIN location. Additionally, this file must have write permissions for the Oracle group so that the db2 instance user ID (which must also be a member of the Oracle group) can update the information for Content Manager.

Oracle NLS message files location

For most customers, this value should be ORACLE_HOME/ocommon/nls/admin/data. It is equivalent to your Oracle ORA_NLS33 environment variable. This setting is intended primarily for customers who have different installations of Oracle on the same machine and utilize different language versions.

Oracle database server version

If you are using any version of Oracle 9.2.0.1 or higher, you should select ″9.2.0.1 or higher″. If you are selecting any version of Oracle 8.1.7.4 or higher, but are not using Oracle 9i, you should select ″8.1.7.4 or higher″. Note that Content Manager does not support Oracle versions of 9i less than 9.2.0.1, nor any versions of 8i less than 8.1.7.4.

Refer to Oracle's Metalink website for any patchsets and related installation instructions you may need to upgrade your Oracle system prior to installing Content Manager.

Password (for Oracle SYS and SYSTEM)

This is the password that will be *set* for the Oracle-created accounts SYS and SYSTEM. At database creation time, these two internal accounts are set with the password value you provide here. As indicated in Oracle security guidelines, you should differentiate the password used for these accounts after database creation. Setting the passwords provides additional security for the administration of your Oracle database.

Library server database administration ID/Schema name

This will be the user ID used to administer your Content Manager library server. In most cases, this will also be your Library server schema name. Therefore, unless you specifically want to have your library server schema ID separate from your library server administrator ID, these two values will be the same (for example: `icmadmin`).

DB2 instance owner ID

This is the user ID you created prior to installation of the DB2 product. It is the user ID that you specified during installation of DB2 as the DB2 instance user ID. It is also the user ID that you included in the Oracle user ID group. As the user ID that owns a DB2 instance, this user ID, by default, also has `DB2 SYSADM` privileges which are needed to create a DB2 federated database that connects to your Oracle data source.

Library server database location

This should be the fully-qualified path name of the location where you want Oracle to store its internal database files. Additionally, this directory will be used by the installation program to generate intermediate files and database creation log files. It keeps a copy of your `icmlsdb.properties` file for future use. If you will be installing the library server application on an Oracle client machine, you should use `ftp` to connect to this file to your Oracle client machine (to save time and provide default values for the library server application installation). If the directory provided in this field does not exist, the installation program creates it for you. If you are using a directory that already exists, you must ensure that it is owned by the Oracle user ID and has write permissions for the Oracle user ID and Oracle group.

Library server host name

This is the host-only name of the Oracle server on which your library server database will be created. If you are installing a library server database, this will be the host name for the local Oracle server machine. If you are installing the library server application, this will be the host name for the Oracle server machine that *already* contains your library server database.

Oracle listener name

For most Oracle installations, and the value provided by default during an Oracle installation, you will never need to specify a value other than LISTENER. If, however, you are certain that your organization uses named listeners and you want to use a specific listener, please enter that name in this field. You can check to see the name of the current, active listener on your Oracle server by issuing the following command:

```
lsnrctl status
```

If the active listener is not the listener you wish to use, you can check your `listener.ora` file on the Oracle server to determine which available, named listener you wish to use. If you want to create a new listener, the listener must be added to your `listener.ora` file before beginning Content Manager installation.

For proper operation of Content Manager, the listener name you specify in this field must be the active listener on your Oracle server at all times.

Oracle protocol

In most cases, you should accept the default value of TCP/IP for the Oracle communications protocol to be used. If you choose to select another Oracle-supported protocol, you must verify that your Oracle client/server environment is correctly configured for this protocol using the Oracle TNSNAMES naming method and the Oracle Net8 database communications protocol.

Oracle listener port

Most Oracle installations use a default listener port of 1521. If you know that the named listener you wish to use has a different protocol, please specify that value here. You can verify this by referring to your Oracle `listener.ora` file.

Oracle database administration ID

To maximize the security of your library server database and Oracle system, it is good practice to choose a different value for this field than the user ID and password that you provide for the library server administrator user ID and password. This user ID owns the Oracle database and tables and is created as an internal Oracle user only. DB2 Relational Connect does not support the use of other Oracle external authentication methods. Therefore, this user ID MUST remain an internal, Oracle-authenticated user ID. Users can change the Oracle user ID associated with the library server database after installation by running the Content Manager user mapping utility, `icmsumap` for Sun platforms. However, you must ensure that the new user ID has identical Oracle permissions to the previous user ID in use. You should not change this value once Content Manager has been installed, but instead change only the password associated with the user, unless your organization's security policy dictates otherwise.

Password (for Oracle database administration ID)

This value should not be the same value used for your library server administrator password. This is to maximize the security of your library server database and Oracle system.

Mirror directory

If you choose to use this Oracle mirroring option, it enables Oracle to mirror the Oracle log files (useful for recovery purposes). Refer to your Oracle server documentation for more information about mirroring.

Resource manager database location

This should be the fully-qualified path name of the location where you want Oracle to store its internal database files. Additionally, this directory will be used by the installation program to generate intermediate files and database creation log files. It keeps a copy of your `icmrmdb.properties` file for future use. If you will be installing the resource manager application on an Oracle client machine, you should use `ftp` to connect to this file to your Oracle client machine (to save time and provide default values for the library server application installation). If the directory provided in this field does not exist, the installation program creates it for you. If you are using a directory that already exists, you must ensure that it is owned by the Oracle user ID and has write permissions for the Oracle user ID and Oracle group.

Resource manager host name

This is the host-only name of the Oracle server on which your resource manager database will be created. If you are installing a resource manager database, this will be the host name for the local Oracle server machine. If you are installing the resource manager application, this will be the host name for the Oracle server machine that *already* contains your resource manager database.

Chapter 19. Verifying a successful installation of Content Manager on AIX

Use information in this section to verify a successful installation of Content Manager on an AIX system:

Verify library server database

To verify that the library server is installed correctly:

__ 1. Check database connection by typing:

```
 # db2 connect to icmnlsdb user icmadmin using password
```

You should see output similar to the following:

```
Database Connection Information
Database server        = DB2/6000 7.2.4
SQL authorization ID   = ICMADMIN
Local database alias   = ICMNLSDB
```

__ 2. Check database tables by typing:

```
# db2 list tables
```

You should see several tables listed (around 125); some with names starting with ″FA″ and some starting with ″ICM″. For Oracle: you will not see any tables with names starting with ″FA″. You will only see tables with names starting with ″ICM″.

__ 3. You can also check $ICMROOT/config/icmcrlsdb.log and search for the term ″SQLSTATE″ to find error messages. This file may be in the **logs** directory rather than the **config** directory if the errors were detected during the installation. A few of the SQLSTATE messages are normal and you need to read the surrounding text to determine if there may have been a problem. For example, you should expect to find SQLSTATE=08003 messages in the log after the CONNECT RESET commands.

For Oracle only: Log files generated during Oracle database creation will be in the "Library server database location" specified during install, ending with the suffix .log. Log files generated during DB2 database creation will be in the /tmp directory, icmlscrdb.db2.log.

If database creation fails, you should verify the values used in your icmlsdb.properties file. For Oracle database creation, this file will be located in the "Library server database location" specified during installation. For DB2 database creation, this file will be located in the /tmp directory. If one of the values in the properties file is incorrect, you can edit the file with vi or other similar editor to correct the value. Once you are satisfied that the properties file is correct, re-run the installation program and browse to the directory where their properties file is located. You should also verify your tnsnames.ora, listener.ora, and sqlnet.ora on your Oracle server using the methods already described. The sqlnet.ora file on the Oracle client machine should use the same settings described earlier for the Oracle server.

Verify library server access modules generated

To verify that the library server access modules were generated correctly:

__ 1. Look for *.DLL files in:

```
/home/db2fenc1/ICMNLSDB/DLL
```

If the DLLs are not there, then your compiler environment settings may not be set up correctly for Content Manager. You may find some .tx3 files in the /home/db2fenc1/ICMNLSDB/DLL directory instead which will contain error messages.

Confirm that you are using the VisualAge C++ compiler v5.0. Make sure the ICMCOMP environment variable is set to /usr/vacpp/bin

In the *tx3 files, if you see compilation errors indicating the SQL header files cannot be found (e.g. SQLDA), execute the following command to create the symbolic links for DB2:

```
 # /usr/lpp/db2_07_01/cfg/db2ln
```

After you determine the cause of the compilation problems identified in the .tx3 files, you can regenerate the access modules by executing:

```
# cd /usr/lpp/icm/config
# java TRebuildCompTypeICM ICMNLSDB icmadmin password
            ICMADMIN /tmp/run.out
# java ICMDefineSystemItemTypes ICMNLSDB icmadmin password
            ICMADMIN /tmp/run.out
```

__ 2. Look in the /usr/lpp/icm/logs/icm81install.log make sure you see the following output:

```
Generating DLL for access module: ICMNLSDB icmadmin ...
Number of views found: 16
Generating access module for view with ID: 200
Generating access module for view with ID: 201
Generating access module for view with ID: 202
Generating access module for view with ID: 203
Generating access module for view with ID: 204
Generating access module for view with ID: 205
Generating access module for view with ID: 206
Generating access module for view with ID: 207
Generating access module for view with ID: 208
Generating access module for view with ID: 300
Generating access module for view with ID: 301
Generating access module for view with ID: 302
Generating access module for view with ID: 303
Generating access module for view with ID: 304
Generating access module for view with ID: 400
Generating access module for view with ID: 500
All access modules rebuilt
```

This output confirms successful generation of the access module stored procedures. The access modules are used for Content Manager item types. They are dynamically generated using the C++ compiler.

If the access modules are not correctly built:

- You will have problems loading documents
- You will see a message in the log file (see *Messages and Codes* documentation for the name and location of the log file for the component you are using):

  ```
  ICM7007: The access module required to access a component
  table has not been built correctly. The server log contains the
  name of the access module and the component type that must be
  built.
  Delete and re-create the item type and verify the access module
  is correctly built.
  (STATE) : [LS RC = 7007] com.ibm.mm.sdk.common.
  DKUsageError: DGL3608A: DLL not ready;

  ICM7007: The access module required to access a component table
  has not been built correctly. The server log contains the name
  of the access module and the component type that must be built.
  Delete and re-create the item type and verify the access module
  is correctly built.
  (STATE) : [LS RC = 7007]
  ```

  If you encounter this error, delete the `$ICMDLL/ICMNLSDB` directory (for example: `/home/db2fenc1/ICMNLSDB`), then run **TRebuildCompTypeICM** described above.

Verify that the library server monitor program is running

To verify that the library server monitor is running, use the procedure for “Running the library server monitor program” on page 498.

Verify resource manager database

To verify that the resource manager is installed correctly:

__ 1. If you have not done so, execute the following:

```
# . /home/db2inst1/sqllib/db2profile
```

__ 2. Check database connection by typing:

```
# db2 connect to rmdb user rmadmin using password
```

You should see output similar to the following:

```
    Database Connection Information

Database server        = DB2/6000 7.2.5
SQL authorization ID   = RMADMIN
Local database alias   = RMDB
```

__ 3. Check database tables by typing:

```
db2 list tables
```

You should see a few tables listed (around 26).

You can also check `$ICMROOT/config/icmcrrmdb.log` and search for the term ″SQLSTATE″ to find error messages. A few of the SQLSTATE messages are normal and you need to read the surrounding text to determine if there may have been a problem. For example, you should expect to find SQLSTATE=08003 messages in the log after the CONNECT RESET commands. This file may be in the logs directory rather than the config directory if the errors were detected during the installation.

Verify resource manager Web application deployment

Follow these steps to verify that the resource manager Web application is deployed correctly for either:

“Advanced Single Server Edition (AES)”

OR

“Advanced Edition (AE)” on page 286

Advanced Single Server Edition (AES)

To verify that the resource manager was deployed correctly with AES:

__ 1. Stop and restart the following services to make sure that the changes made to the HTTP Server and WAS become effective:

__ a. **Stop the HTTP Server**

```
/usr/HTTPServer/bin/apachectl stop
```

__ b. **Start the HTTP Server**

```
/usr/HTTPServer/bin/apachectl start
```

__ c. **Stop WAS Application Server**

```
/usr/WebSphere/AppServer/bin/stopServer.sh
-configFile/usr/lpp/cmb/cmgmt/IDM_ICM.xml
```

OR

```
stopIDMAES.sh in /opt/CMeClient/Save/
```

(default install location on AIX)

__ d. **Start WAS Application Server**

```
/usr/WebSphere/AppServer/bin/startServer.sh
-configFile /usr/lpp/cmb/cmgmt/IDM_ICM.xml
```

OR

```
startIDMAES.sh in /opt/CMeClient/Save/
```

(default install location on AIX)

__ 2. **Regenerate the plug-in configuration:**

__ a. Open a browser, and enter the following URL:

```
http://<hostname>:9090/admin
```

where <hostname> is the fully qualified host name for your WAS machine.

__ b. Configure AES:

1) Click **Configuration**.

2) Click **Open a configuration file to edit with the console**.

3) Select **Enter full path to file on server**.

4) Enter `/usr/lpp/icm/cmb/cmgmt/IDM_ICM.xml`

__ c. Open up the

```
+ Nodes
   +  <hostname> (e.g. homer.stl.ibm.com)
        + Application Servers
             - Default Server
```

in the topology tree in the left pane.

In the right pane, you'll see **Application Servers: Default Server**

__ d. Under **Advanced Settings**, click **Web Server Plug-in Configuration**.

__ e. Click the **Generate** button.

__ f. After completion, you see a couple of message at the top, including:

```
New plug-in configuration has been generated.
```

Click **OK**.

__ g. Click **Configuration needs to be saved**.

__ h. Save to the following file:

```
/usr/WebSphere/AppServer/config/server-cfg.xml
```

__ i. Click **OK**

__ j. This step checks to see that the <icmrm> web application is listed in the WAS Admin Console.

Notice: icmrm is the default name and will be different if you changed it during the install.

In the WAS Admin Console, locate the Resource Manager application (icmrm)

__ k. Select **Enterprise Applications** in the topology tree in the left pane of the WAS Admin Console.

In the right pane, you will see a list of the deployed applications.

__ l. Start the Resource Manager:

__ 1) Click in the check box in front of **icmrm**

__ 2) Press the **Start** button

__ 3. **Validate the deployment:**

__ a. Look for the ICMRM web application in the WAS Admin Console.

__ b. Also check to see if the icmrm files have been copied to the WAS directory, e.g.:

```
/usr/WebSphere/AppServer/installedApps/icmrm.ear/
```

You should see output similar to the following:

```
 Auth Id  Application   Appl.      Application Id              DB     # of
          Name          Handle                                 Name  Agents
-------  ------------ ----------- ---------------------------- ----- ------
RMADMIN  java          35         *LOCAL.db2inst1.020627185929  RMDB    1
RMADMIN  java          36         *LOCAL.db2inst1.020627185931  RMDB    1
RMADMIN  java          37         *LOCAL.db2inst1.020627185932  RMDB    1

   Note the three java.exe processes related to RMDB.
```

Advanced Edition (AE)

To verify that the resource manager was deployed correctly with AE:

__ 1. Stop and restart the following services to make sure that the changes made to the HTTP Server and WAS become effective:

  __ a. **Stop the HTTP Server**

```
/usr/HTTPServer/bin/apachectl stop
```

  __ b. **Start the HTTP Server**

```
/usr/HTTPServer/bin/apachectl start
```

  __ c. **Stop WAS Application Server**

```
/usr/WebSphere/AppServer/bin/wscp.sh -c "Node stop
            /Node:<node_name>/"
```

  Where <node_name> is the name of the node to stop.

  __ d. **Start WAS Application Server**

```
/usr/WebSphere/AppServer/bin/startupServer.sh
```

__ 2. **Regenerate the plug-in configuration**

  __ a. Start the WAS Admin console:

```
/usr/WebSphere/AppServer/bin/adminclient.sh
```

  __ b. Open up the

```
  - WebSphere Administrative Domain
     - Nodes
         +  <hostname> (e.g. homer.stl.ibm.com)
```

  in the topology tree in the left pane.

  __ c. Right click on the hostname and select **Regen Webserver Plugin** from the menu.

  In the message pane at the bottom, you'll see:

```
ADGU1077I: Plugin regeneration completed successfullly...
```

  __ d. In the WAS Admin Console, locate the Resource Manager application (icmrm)

  (This step checks to see that the <icmrm> web application is listed in the WAS Admin Console. **Remember:** that icmrm is the default name and will be different if you changed it during the installation.)

  __ e. Under your hostname, under Nodes, expand to see the **Application Servers** in the topology tree in the left pane of the WAS Admin Console.

  __ f. Start the Resource Manager:

    __ 1) Right mouse button click on the icmrm appserver

    __ 2) From the menu, select **Start**

    __ 3) In WAS AE check RM processes are running by typing:

```
# db2 list applications
```

__ 3. **Validate the deployment:**

__ a. Look for the ICMRM web application in the WAS Admin Console.

__ b. Also check to see if the icmrm files have been copied to the WAS directory, for example:

```
/usr/WebSphere/AppServer/installedApps/icmrm.ear/
```

You should see output similar to the following:

```
 Auth Id  Application   Appl.     Application Id              DB    # of
          Name          Handle                                Name  Agents
-------  ------------ ----------- --------------------------- ----- ------
RMADMIN  java          35         *LOCAL.db2inst1.020627185929  RMDB    1
RMADMIN  java          36         *LOCAL.db2inst1.020627185931  RMDB    1
RMADMIN  java          37         *LOCAL.db2inst1.020627185932  RMDB    1

   Note the three java.exe processes related to RMDB.
```

Verify resource manager Web application in a Web browser

To verify that the resource manager Web application in a Web browser:

__ 1. Start your WebSphere Application Server if it is not already started.

__ 2. Open a web browser and type in the following web addresses:

__ a. `http://<hostname>/icmrm/snoop`

Where `<hostname>` is the fully qualified hostname of your WAS machine. For example, if `homer.svl.imb.com` is your hostname, you would type:

```
http://homer.svl.imb.com/icmrm/snoop
```

You should see the snoop information, which displays network settings for your machine.

__ b. `https://<hostname>/icmrm/snoop`

You should see the snoop information again. The test with https will test your SSL connection.

For more information about the SSL configuration, see "Configure Secure Sockets Layer (SSL) for IBM HTTP server" on page 237.

Troubleshooting note for WAS AE: If you are unable to view the snoop information, look at the WAS configuration file to see if icmrm was deployed to a different port. This may happen if the default port is already used. View /usr/WebSphere/AppServer/config/plugin-cfg.xml. Look for information similar to:

```
<ServerGroup Name="homer/ICMRM">
        <Server CloneID="tr20agvt" Name="ICMRM">
            <Transport Hostname="homer" Port="9081" Protocol="http"/>
        </Server>
```

Notice that Port identifies **9081** (a number other than 9080), if this is the case, then add the port 9081 to your virtual host in the WAS admin console.

__ 1. Under WebSphere Administrative Domains, select **Virtual Hosts**.

__ 2. In the right pane, you see the **Hosts Alias**.

__ 3. Click **Add** to add the new port number.

First Steps

The Content Manager First Steps program allows you to load sample data into the Content Manager servers. You perform the First Steps procedures differently depending whether you have all of the Content Manager components on one system or if you have them installed on more than one system.

For an AIX installation of a library server or a resource manager (or both) you need to run the First Steps program from the Windows system where you installed your system administration client component. See "Running First Steps for a multiple machine Content Manager system" on page 158.

Verifying that DB2 Universal Database Relational Connect is set up correctly for Oracle

After the software is installed, a user with SYSADM authority should check the setup and create the federated database. The DB2 instance owner then configures the server to access the Oracle data sources.

Checking the federated server setup

After the federated server is set up, you can avoid potential problems by checking several key settings:

- Confirm the link between DB2 and the data source client libraries.
- Check the wrapper library file permissions.
- Ensure that the FEDERATED parameter is set to YES.

Checking the data source environment variables

When you set up the federated server, the installation process attempts to set the environment variables for the Oracle Server data sources.

Prerequisites:

A federated server that is properly set up to access your data sources. This includes the installation and configuration of any required software, such as: the client software and DB2 Relational Connect.

Procedure:

Check to make certain that the environment variables for the data sources you want access are set in the `sqllib/cfg/db2dj.ini` file.

The system administrator should check the data source environment variables.

The following table lists the valid environment variables for Oracle.

Table 111. Valid data source environment variables.

Data source	Valid environment variables
Oracle	ORACLE_HOME ORACLE_BASE ORA_NLS TNS_ADMIN

The data source environment variables will not be set in the `sqllib/cfg/db2dj.ini` file if you:

- Install the data source client software after the DB2 federated server is setup.
- Have not installed the data source client software.

To set the environment variables:

__ 1. Install the client software (if necessary).

__ 2. Set the environment variables. The quickest way to set the data source environment variables is:
   - Run the DB2 Relational Connect installation again.

You can also manually set the environment variables.

Manually setting the Oracle environment variables

To manually set the Oracle environment variables, follow these steps:

__ 1. Edit the `db2dj.ini` file located in `sqllib/cfg` directory. The `db2dj.ini` file contains configuration information about the Oracle client software installed on your federated server. If the file does not exist, you can create a new file with this name. In the `db2dj.ini` you must specify the fully qualified path for the variable, otherwise you will encounter errors. Set the following environment variables as necessary.

ORACLE_HOME

Set the ORACLE_HOME environment variable to the directory path where the Oracle client software is installed. Specify the fully qualified path for the variable, ORACLE_HOME=<oracle_home_directory>. For example, if the Oracle home directory is `/usr/oracle/8.1.7`, the entry in the `db2dj.ini` is:

```
ORACLE_HOME=/usr/oracle/8.1.7
```

Note: If an individual user of the federated instance has the ORACLE_HOME environment variable set, federated instance does not use that setting. The federated instance uses only the value of ORACLE_HOME that you set in the DB2 profile registry.

ORACLE_BASE

ORACLE_BASE represents the root of the Oracle client directory tree. If you set the ORACLE_BASE variable when you installed the Oracle client software, set the ORACLE_BASE environment variable on the federated server. For example:

```
ORACLE_BASE=<oracle_root_directory>
```

ORA_NLS

If your system is using multiple versions of Oracle, you must ensure that:

- The appropriate ORA_NLS variable is set.
- The corresponding NLS data files for the versions you are using are available.

The location-specific data is stored in a directory specified by the ORA_NLS environment variable. For each new version of Oracle, there is a different ORA_NLS data directory.

Table 112. Oracle ORA_NLS directory name, by version.

Oracle version	Environment variable
7.2	ORA_NLS
7.3	ORA_NLS32
8.0, 8.1, 9.0.1	ORA_NLS33

For example, for federated servers that access Oracle 8.1 data sources, set the ORA_NLS environment variable:

```
ORA_NLS32=<oracle_home_directory>/ocommon/nls/admin/data>
```

TNS_ADMIN

The Oracle client expects to locate the tnsnames.ora file in the /NETWORK/ADMIN directory. The client will also look for the tnsnames.ora file in the /etc directory. If the tnsnames.ora file is not located in one of these directories, you need to set the TNS_ADMIN environment variable on the federated server. For example:

```
TNS_ADMIN=<tnsnames.ora_directory>
```

__ 2. Update the .profile file of the DB2 instance with the Oracle environment variable. You can do this by issuing the following command:

```
export PATH=$ORACLE_HOME/bin:$PATH
export ORACLE_HOME=<oracle_home_directory>
```

where <oracle_home_directory> is the directory where the Oracle client software is installed.

__ 3. Execute the DB2 instance .profile by entering:

```
. .profile
```

__ 4. Ensure that the environment variables are set on the federated server, by recycling the DB2 instance. Issue the following commands to recycle the DB2 instance:

```
db2stop
db2start
```

Confirming the link between DB2 and the data source client libraries

A federated server must be link-edited to the data source client libraries. The link-edit step is attempted when you install DB2 Relational Connect.

The link-edit step creates a wrapper library for each data source that the federated server will communicate with.

If the data source client software was not installed before you installed the DB2 server software, the link-edit step will fail. You will then need to perform the link manually.

Prerequisites:

A federated server that is properly setup to access your data sources. This includes the installation and configuration of any required software, such as: the client software, DB2 Relational Connect, or DB2 Life Sciences Data Connect.

Restrictions:

You need root authorization to run the link scripts.

Procedure:

Determine the status of the link between DB2 and the data source client libraries:

- If the link-edit was successful, the wrapper library file appears in the directory.
- If the link-edit failed, check the error message file in the directory.
- If the link-edit was not performed, neither the library file or message file appears in the directory. You will have to manually run the link script.

The following sections contain information on how to confirm the status of the link-edit, and provide instructions on how to perform the links manually.

Checking for the wrapper library files

The link-edit scripts create the wrapper libraries in specific directories, depending on the operating system. The following tables list the directory path for the library file names by data source. If the wrapper library file appears in the directory, the link-edit was successful.

The wrapper library names for Oracle are:

Table 113. Oracle wrapper library names

Operating system on your federated server	Wrapper library names for SQLNET	Wrapper library names for NET8
AIX	libdb2sqlnet.a	libdb2net8.a
Solaris	libdb2sqlnet.so	libdb2net8.so
Windows NT and Windows 2000	db2sqlnet.dll	db2net8.dll

Checking the link-edit error message files

If the link-edit fails, there will be errors listed in the error message file in the library directory. There may be an error message file in the library directory, even if the link-edit is successful. You need to open the error message file to determine if the link-edit failed. The link-edit error message file names are listed in the following table.

Table 114. Link-edit error message file names by data source

Data source	Error message file names
Oracle	djxlinkOracle.out

Manually linking DB2 to the data source client libraries

The link script creates the wrapper libraries on the federated server for the data source you are setting up. There are several reasons why the link might fail when you setup the federated server:

- If the client software is not installed before the link-edit is attempted, then the link-edit will fail.
- Check to make sure the version of the data source client is supported. The latest information is on the product Web sites. Check the DB2 Relational Connect Web sitewww.ibm.com/software/data/db2/relconnect/. If the version of the data source client you have installed is not supported, the link-edit will fail. You will have to install a client version that is supported and then perform the link manually.

You need root authorization to run the link scripts. The quickest way to link DB2 to the data source client libraries is:

__ 1. Install and configure the client software on the DB2 federated server (if necessary).

__ 2. Use the product CDs and run the DB2 Relational Connect installation again.

Alternatively, you can run the link scripts from the command prompt.

The the link script name is `djxlinkOracle`.

Issue the script from the command prompt:

```
djxlinkOracle
```

If you manually run a link script, you must issue the **db2iupdt** command on each DB2 instance to enable federated access to the data sources.

Note: There is another script, the `djxlink` script, that attempts to create a wrapper library for every data source that DB2 supports. If you only have the client software for some of the data sources installed, you will receive an error message for each of the missing data sources when you issue the `djxlink` script.

Once the link is performed, check the permissions on the wrapper libraries after they are created. Make sure that the libraries can be read and executed by the DB2 instance owners.

Creating the federated database

After you setup the federated server, the DB2 instance owner creates a DB2 database on the federated server instance that will act as the federated database.

You can create the database two ways:

- Through the DB2 Control Center
- Through the DB2 Command Center or DB2 command line processor (CLP).

The advantage of using the DB2 Control Center is that you do not have to key in each statement and command. It is the easiest way to quickly create a database.

The steps in this section assume that you are using the DB2 Command Center or the command line processor (CLP) to create the database.

Prerequisites:

A federated server that is properly setup to access your data sources. This includes the installation and configuration of any required software, such as: the client software and DB2 Relational Connect.

Restrictions:

You need SYSADM or SYSCTRL authority to create a DB2 database.

Procedure:

Create a DB2 database on the federated server instance that will act as the federated database. For example:

```
CREATE DATABASE federated
```

This command:

- Initializes a new database.
- Creates the three initial table spaces.
- Created the system tables.
- Allocates the recovery log.

In a multi-node environment, this command affects all nodes that are listed in the `db2nodes.cfg` file. The node from which this command is issued, becomes the catalog node for the new database.

Adding Oracle data sources to a federated server

Configuring the federated server to access Oracle data sources involves supplying the server with information about the Oracle data sources and objects you want to access. You can configure access to Oracle data sources two ways:

- Through the DB2 Control Center
- Through the DB2 Command Center or command line processor (CLP)

The advantage of using the DB2 Control Center is that you do not have to key in each statement and command. It is the easiest way to quickly configure access to Oracle data sources. There are a few configuration tasks that can not be accomplished through the DB2 Control Center:

- Setting up and testing the Oracle client configuration file.
- Testing the connection to the Oracle server to validate the server definition and user mappings.
- Adding or dropping column options.

The steps in this section assume that you are using the DB2 Command Center or the command line processor (CLP) to configure access to Oracle data sources.

Prerequisites:

- A federated server and database that are setup to access Oracle data sources.
- The Oracle client software installed and configured on the federated server.
- The proper variables setup. This includes: system environment variables, db2dj.ini variables (UNIX only), and DB2 Profile Registry (db2set) variables.

Procedure:

To add an Oracle data source to a federated server:

1. Set up and test the Oracle client configuration file.
2. Create the wrapper.
3. Create the server definition and set the server options.
4. Create the user mappings.
5. Test the connection to the Oracle server.
6. Create nicknames for Oracle tables and views.

These steps are explained in detail in this section. Operating system-specific differences are noted where they occur.

Step 1: Set up and test a client configuration file

The client configuration file is used to connect to Oracle databases, using the client libraries that are installed on the federated server. This file specifies the location of each Oracle database server and type of connection (protocol) for the database server. The default name for the Oracle client configuration file is `tnsnames.ora`.

To set up the client configuration file, use the utility that comes with the Oracle client software. See the installation documentation from Oracle for more information about using this utility. Within the tnsnames.ora file, the SID is the name of the Oracle instance, and the HOST is the host name where the Oracle server is located.

The directory in which the tnsnames.ora file is created is $ORACLE_HOME/network/admin .

Test the connection to ensure that the client software is able to connect to the Oracle server. Use the Oracle **sqlplus** tool to test the connection.

Setting a different location for the tnsnames.ora file: If you decide to place the tnsnames.ora file in a path other than the default search path, you must set the TNS_ADMIN environment variable to specify the file location. To set this environment variable:

__ 1. Edit the db2dj.ini file located in the sqllib/cfg directory, and set the TNS_ADMIN environment variable:

```
TNS_ADMIN=x:\path\tnsnames.ora
```

__ 2. To ensure that the environment variable is set in the program, recycle the DB2 instance. Issue the following commands to recycle the DB2 instance:

```
db2stop
db2start
```

Step 2: Create the wrapper

To specify the wrapper that will be used to access Oracle data sources, use the CREATE WRAPPER statement. DB2 Relational Connect includes two wrappers for Oracle — SQLNET and NET8. To determine which wrapper to use, consult the following table.

Table 115. Oracle wrappers by client version and operating system

Oracle client	Operating system	Wrapper to use
Oracle Version 7	AIX	SQLNET
	Windows NT and Windows 2000	SQLNET
	Solaris	not applicable
Oracle Version 8	AIX	NET8
	Windows NT or Windows 2000	NET8 (recommended) or SQLNET
	Solaris	NET8

Table 115. Oracle wrappers by client version and operating system (continued)

Oracle client	Operating system	Wrapper to use
Oracle Version 9	AIX	NET8
	Windows NT or Windows 2000	NET8 (recommended) or SQLNET
	Solaris	NET8

Note: The SQLNET wrapper uses OCI 7 (Oracle Call Interface) API calls. The NET8 wrapper uses OCI 8 API calls. If the Oracle 8 or Oracle 9 client is installed, you will experience better performance and functionality by using the NET8 wrapper. Additionally, the NET8 wrapper has LOB support. Because the OCI 7 does not support LOB data types, the SQLNET wrapper does not support Oracle LOB data types.

- The SQLNET wrapper maps Oracle LONG data types to DB2 for UNIX and Windows LOB data types.
- The NET8 wrapper does not support Oracle LONG data types. It does map Oracle LOB data types to DB2 for UNIX and Windows LOB data types.

The following example shows the CREATE WRAPPER statement for the NET8 wrapper:

```
CREATE WRAPPER NET8
```

Recommendation: Use the default wrapper names (SQLNET or NET8). When you create the wrapper using one of the default names, the federated server automatically picks up the default library name associated with the wrapper. If the wrapper name conflicts with an existing wrapper name in the federated database, you can substitute the default wrapper name with a name you choose. If you use a name that is different than one of the default names, you must include the LIBRARY parameter in the CREATE WRAPPER statement.

Suppose that you have a federated server running on AIX and you decide to use a wrapper name that is not one of the default names. Examples of the CREATE WRAPPER statements for SQLNET and NET8 are:

```
CREATE WRAPPER mywrapper LIBRARY 'libdb2sqlnet.a'
```

```
CREATE WRAPPER mywrapper LIBRARY 'libdb2net8.a'
```

The wrapper library names for Oracle are:

Table 116. Oracle wrapper library names

Operating system on your federated server	Wrapper library names for SQLNET	Wrapper library names for NET8
AIX	libdb2sqlnet.a	libdb2net8.a

Table 116. Oracle wrapper library names (continued)

Operating system on your federated server	Wrapper library names for SQLNET	Wrapper library names for NET8
Solaris	libdb2sqlnet.so	libdb2net8.so
Windows NT and Windows 2000	db2sqlnet.dll	db2net8.dll

Step 3: Create the server definition

In the federated database, you must define each Oracle server that you want to access. You create a server definition using the CREATE SERVER statement. For example:

```
CREATE SERVER oraserver TYPE oracle VERSION 7.2 WRAPPER net8
OPTIONS (NODE 'paris_node')
```

oraserver
: A name that you assign to the Oracle database server. This name must be unique. Duplicate server names are not allowed.

TYPE *oracle*
: Specifies the type of data source server to which you are configuring access. The type parameter for the SQLNET and NET8 wrappers must be *oracle*.

VERSION *7.2*
: The version of Oracle database server that you want to access. The supported Oracle versions are 7.x, 8.x, and 9.x.

WRAPPER *net8*
: The name you specified in the CREATE WRAPPER statement.

NODE *'paris_node'*
: The name of the node where the Oracle database server resides. Obtain the node name from the tnsnames.ora file.

Although the node name is specified as an option in the CREATE SERVER statement, it is required for Oracle data sources.

Locating the node name: You must define the node name in the Oracle tnsnames.ora file (see step 1). Although the *node_name* is specified as an option in the CREATE SERVER statement, it is required for Oracle data sources. This is an example of a tnsnames.ora file:

```
ORA9I.SEEL =
  (DESCRIPTION =
  (ADDRESS_LIST =
     (ADDRESS = (PROTOCOL = TCP)(HOST = somehost)(PORT = 1521)))
     (CONNECT_DATA =
     (SERVICE_NAME = ora9i.seel)))
```

The node value to use in the CREATE SERVER statement would be `ora9i.seel`.

Optional: Set additional server options: When you create the server definition, you can specify additional server options in the CREATE SERVER statement. There are general server options and data source-specific server options.

DB2 assumes that all of the Oracle VARCHAR columns contain trailing blanks. If you are certain that all VARCHAR columns in the Oracle database do not contain trailing blanks, you can set a server option to specify that the data source uses a non-blank padded VARCHAR comparison semantic. An example of the CREATE SERVER statement with this server options is:

```
CREATE SERVER oraserver TYPE oracle VERSION 7.2 WRAPPER net8
OPTIONS (NODE 'paris_node', VARCHAR_NO_TRAILING_BLANKS 'Y')
```

Use the VARCHAR_NO_TRAILING_BLANKS server option when all the columns do not contain trailing blanks. If only ssome of the VARCHAR columns do not contain trailing blanks, you can set an option on those specific columns with the CREATE NICKNAME or ALTER NICKNAME statements.

After the server definition is created, use the ALTER SERVER statement to add or drop server options.

Step 4: Create the user mappings

When you attempt to access an Oracle server, the federated server must first establish a connection to the data source. The federated server does this by using a valid user ID and password to that data source. You must define an association between the federated server user ID and password and the data source user ID and password. This association must be created for each user ID that will be using the federated system to send distributed requests. This association is called a *user mapping*.

Use the CREATE USER MAPPING statement to map the local user ID to the Oracle server user ID and password; for example:

```
CREATE USER MAPPING FOR robert SERVER oraserver
OPTIONS (REMOTE_AUTHID 'rob', REMOTE_PASSWORD 'then4now')
```

robert The local user ID that you are mapping to a user ID defined at an Oracle server.

SERVER *oraserver*
The name of the Oracle server that you defined in the CREATE SERVER statement.

REMOTE_AUTHID *'rob'*
Tthe user ID at the Oracle database server to which you are mapping

robert. This value is case sensitive unless you set the FOLD_ID server option to ’U’ or ’L’ in the CREATE SERVER statement.

REMOTE_PASSWORD *’then4now’*
: The password associated with *’rob’*. This value is case sensitive unless you set the FOLD_PW server option to ’U’ or ’L’ in the CREATE SERVER statement.

You can use the DB2 special register **USER** to map the authorization ID of the person issuing the CREATE USER MAPPING statement to the data source authorization ID specified in the **REMOTE_AUTHID** user option. The following is an example of the CREATE USER MAPPING statement which includes the **USER** special register:

```
CREATE USER MAPPING FOR USER SERVER oraserver
OPTIONS (REMOTE_AUTHID 'rob', REMOTE_PASSWORD 'then4now')
```

Restriction: The user ID at the Oracle data source must have been created using the Oracle create user command with the ’identified by’ clause, instead of the ’identified externally’ clause.

Step 5: Test the connection to the Oracle server

Test the connection to the Oracle server to ensure that you can establish a connection, using the server definition and user mappings you defined. Open a pass-through session and issue a SELECT statement against the Oracle system tables. For example:

```
SET PASSTHRU server_name
SELECT count(*) FROM sys.all_tables
SET PASSTHRU RESET
```

If the SELECT returns a count, then your server definition and user mapping are set up properly. If the SELECT returns an error, you might have to:

- Check the Oracle server to make sure that it is configured for incoming connections.
- Check your user mapping to make sure that the settings for the REMOTE_AUTHID and REMOTE_PASSWORD options are valid for connections to the Oracle server.
- Check the Oracle client software on the DB2 federated server to make sure that it is installed and configured correctly to connect to the Oracle server.
- Check your DB2 federated variables to make sure that they are correct for working with the Oracle server. This includes checking the system environment variables, db2dj.ini variables, and the DB2 Profile Registry (db2set) variable.
- Check your server definition and possibly drop it and create it again.
- Check your user mapping and possibly alter it or create another if necessary.

Step 6: Create the nicknames for tables and views

The federated database relies on catalog statistics for nicknamed objects to optimize query processing. These statistics are gathered when you create a nickname for a data source object using the CREATE NICKNAME statement. The federated database verifies the presence of the object at the data source, and then attempts to gather existing data source statistical data. Information useful to the optimizer is read from the data source catalogs and put into the global catalog on the federated server. Because some or all of the data source catalog information might be used by the optimizer, update statistics (using the data source command equivalent to RUNSTATS) at the data source before you create a nickname.

For each Oracle server you defined, assign a nickname to each table or view you want to access on those servers. You will use these nicknames, instead of the names of the data source objects, when you query the Oracle servers. Nicknames can be up to 128 characters in length.

The federated server will fold the Oracle server, schema, and table names to uppercase unless you enclose them in double quotation marks (″). The following example shows a CREATE NICKNAME statement:

```
CREATE NICKNAME PARISINV FOR oraserver."france"."inventory"
```

:

PARISINV

A unique nickname used to identify the Oracle table or view.

Note: the nickname is a two-part name—the schema and the nickname. If you omit the schema when creating the nickname, the schema of the nickname will be the authorization ID of the user creating the nickname.

oraserver."france"."inventory"

A three-part identifier for the remote object:

- *oraserver* is the name you assigned to the Oracle database server in the CREATE SERVER statement.
- *france* is the name of the remote schema to which the table or view belongs.
- *inventory* is the name of the remote table or view that you want to access.

Repeat this step for each Oracle table or view for which you want create nicknames. When you create the nickname, DB2 will use the connection to query the data source catalog. This query tests your connection to the data source using the nickname. If the connection does not work, you will receive an error message.

Tuning and troubleshooting the configuration to Oracle data sources

After you have set up the configuration to Oracle data sources, you may want to modify the configuration to improve performance. For example, you might want to set the DB2_DJ_COMM environment variable to improve performance when the Oracle data source is accessed.

Improving performance by setting the DB2_DJ_COMM environment variable

If you find that it takes an inordinate amount of time to access the Oracle server, you can improve the performance by setting the DB2_DJ_COMM environment variable. Setting the DB2_DJ_COMM environment variable will load the wrapper when the federated server initializes rather than when you attempt to access the data source.

__ 1. Set the DB2_DJ_COMM environment variable to the wrapper library that corresponds to the wrapper that you specified. Suppose that your federated server is running AIX and the wrapper you are using is NET8. The command to set the DB2_DJ_COMM environment variable is:

```
db2db2set DB2_DJ_COMM= 'libdb2net8.a'
```

Consult the following table for the proper library name.

Table 117. Oracle wrapper library names

Operating system on your federated server	SQLNET wrapper library names	NET8 wrapper library names
AIX	libdb2sqlnet.a	libdb2net8.a
Solaris	libdb2sqlnet.so	libdb2net8.so

__ 2. Recycle the DB2 instance to ensure that the environment variables are set in the program. When you recycle the instance, the DB2 instance accepts the changes that you made. Issue the following commands to recycle the DB2 instance:

```
db2stop
db2start
```

Connectivity problems

For each HOST in the DESCRIPTION section of the `tnsnames.ora` file, you might need to update the `hosts` file:

```
/etc/hosts
```

Whether you update this file depends on how TCP/IP is configured on your network. Part of the network must translate the remote host name specified in the DESCRIPTION section in the `tnsnames.ora` file to an address. If your network has a named server that recognizes the host name, you do not need to update the TCP/IP `hosts` file. Otherwise, you need an entry for the remote host. See your network administrator to determine how your network is configured.

Chapter 20. Installing Enterprise Information Portal components on AIX

This section explains how to install EIP components on AIX servers. You can install all of the Enterprise Information Portal components, except for the administration client, on AIX.

You can install the components only through the installation wizard. Installation through `smitty` or through `installp` is not recommended, because installation also requires configuration.

Installing Enterprise Information Portal components on AIX

To install the AIX components:

1. Perform all the tasks described in Chapter 17, "Performing pre-installation steps on AIX", on page 235.
2. Mount the Enterprise Information Portal installation CD.
3. Change to the CD ROM directory: `cd/ cdrom`
4. Change directory to `release/` and type:

   ```
   ./frnxsetup.sh
   ```

   to launch the installation program.
5. Click **Next** to close the Welcome window.
6. Select the required components and subcomponents. By default, all the components and subcomponents are selected. Type data in the installation windows. See "EIP AIX installation windows" for more information.
7. Follow program prompts to define the settings for the selected components.
8. Click Finish when the Installation Completion window is displayed.
9. Configure the environment variables and classpath (see "Exporting classpath, environment variables on AIX" on page 314)

EIP AIX installation windows

This section describes the AIX installation windows in sequential order. **Tip:** You might not see all the windows. For example, if you do not install the Text Search client, you will not see the two windows associated with the Text Search client.

Component Selection

Select the components and subcomponents and click **Next**. You can install all components at the same time, or select individual components or install all components at the same time.

System Configuration

EIP Version 8 offers a new option that allows remote EIP components to access system configuration files across a network or Web server.

The default installation for common configuration files is:

```
CM_COMMON=/usr/lpp/cmb/cmgmt
```

The selections you make on the System Configuration window define the location of the system configuration files. For example, the configuration file `cmbicmsrvs.ini` contains data required to connect to and search a Content Manager Version 8 server. The window also gives you the option to point remote components to a datasource file stored on an LDAP server.

Restrictions

- The configuration files do not have to be installed on the network or Web server when you define the path, but the files must be installed before remote users can work with EIP. To install the configuration files on a network or Web server, you can use the EIP installation CD-ROM, or, if you have already installed configuration files on another server, you can copy the `cmgmt` directory to the network or Web server.
- Before remote EIP components can access and use configuration files on a network server, you must configure the following properties:
  - Set up sharing on the configuration file directories and subdirectories.
  - Define user IDs and passwords for the remote users on the server where you installed the shared configuration files.
  - Be sure the user IDs and passwords have read/write privileges. Read/write access is required because the clients and other components update shared configuration files, including log files.
- If you install the configuration files on a Web server, see the Web administrator for information on configuring sharing and read/write parameters for remote EIP users.
- If you are installing the Information Center, you must select Local to install the system configuration files. The Information Center files are installed in `/usr/lpp/infoctr`. Users cannot access the Information Center through a network or Web server.
- If you plan to point remote users to datasource configuration information stored on an LDAP server, you must use a utility specific to your LDAP

product to install only the datasource configuration file. See your LDAP administrator for more information. The datasource file is named `cmbds.ini`.

- The option to point remote users to a datasource file stored on an LDAP server is only selectable if:
  - You are installing the Content Manager Version 8 connector and
  - You are installing the federated connector by itself and/or
  - You are installing the administration database, or the Information Mining database, because the federated connector is always installed with those components.

This section describes the fields on the System Configuration window.

Local Click Local to install the configuration files on the local server.

Remote

Click Remote and type the path where you installed, or plan to install, the configuration files on a network server.

Tip: If you have already installed, or plan to install, Content Manager Version 8, EIP can share the Content Manager configuration files across a network. Click Remote and type in the path where you installed or plan to install the Content Manager configuration files.

HTTP web server

Type the URL of the Web server where you installed, or plan to install, the configuration files. The configuration files do not have to be installed on the Web server when you type the URL, but they must be installed before remote users can work with EIP. Contact the Web administrator to learn more about how remote EIP users can connect to and update configuration files on a Web server.

Tip: If you have already installed, or plan to install, Content Manager Version 8, EIP can share the Content Manager configuration files. Type the URL where you installed or plan to install the Content Manager Version 8 configuration files.

Use system configuration

Click this box to begin the process of defining and configuring LDAP server information so you can later install the `cmbds.ini` configuration file. If you click this box and press **Next**, the installation program displays the **Define LDAP Server** and **Configure LDAP Server** windows. The information you define those two windows is stored in the `cmbcmenv.properties` file for later use by EIP components. **Tip**: the installation program detects an existing `cmbcmenv.properties` file, you will not be able to modify any of the fields in Define LDAP Server and Configure LDAP Server windows.

You install the configuration files on the LDAP server in a separate step using an LDAP utility after you install EIP. For more information, see the LDAP server documentation.

You see **Define LDAP Server** and **Configure LDAP Server** only if you:

- Click LDAP server on the System Configuration window and
- Install the Content Manager Version 8 connector and
- Install the federated connector either by itself of as part of an administration or Information Mining database

Define LDAP Server

On this window, you define the LDAP server type, host name, port and authentication methods. EIP stores the information you type in this window in `cmbenv.properties`. **Tip:** You are not required to install, configure or start any LDAP servers before you define the information required on this window.

LDAP server type
Select IBM Secureway or Microsoft Active Directory

Host name
Type the LDAP server host name.

Port number
Type the LDAP server port number.

LDAP server administration ID
Type the LDAP administration user ID.

Password
Type the LDAP administration password.

Configure LDAP Server

On this window, you define the LDAP Server Base distinguished name and User authentication attributes, search scope and referral method.

Base distinguished name
Type the base distinguished name of the organization and country.

User authentication attribute
Type the attribute, for example, `uid`

Search scope
Click Subtree or Onelevel.

Referral
Click Ignore or Follow.

Confirm LDAP Server Setup Information

This window displays the values you typed in the Define LDAP Server and Configure LDAP Server windows. Click **Next** to accept the data, or click **Back** to modify the data.

Configure Content Manager V8 Server Connection

On this window, you define the information required to connect to the Content Manager Version 8 server. You only see this window if you install the Content Manager Version 8 connector. When the administrator defines and connects to a Content Manager Version 8 server, EIP uses the values you define in this window to connect to the server. By default, EIP copies the information from this window to `cmbicmsrvs.ini` and `cmbicmenv.ini`.

Database name
Type the Content Manager Version 8 database name. If you have cataloged the database, type the alias name in this field.

Schema name
Type the schema name that was assigned to the Content Manager Version 8 database when the database was installed.

Authentication type
If you leave the default setting of Server, then the Content Manager Version 8 database user ID and password is sent to the Content Manager Version 8 server for validation.

If you click Client, no validation is performed by DB2, and the user ID you type to log in to your system allows connection to the Content Manager Version 8 Library Server. **Restriction:** when you log in to the client workstation, you must enter a user ID that has DB2 connect privileges.

Database connection ID
You must type the same user ID and password that was defined as the Database connection ID when the Content Manager Version 8 Library Server database was installed.

Enable sign-on
Click True to enable single sign-on, if required by your EIP system plan.

Content Manager V8 Connector: Confirm Server Setup Information

This window displays the values you typed to configure the Content Manager Version 8 connectivity information.

Click **Next** to accept the values, or click **Back** to modify the values.

Configure Federated Connection

On this window, you define the information required to connect an administration client to the administration database. You see this window if you choose any connector, or if you install the administration client. EIP copies the information from this window to a configuration file named `cmbds.ini` and `cmbfedenv.ini`.

Database name
Type the administration database name.

Schema name
Type the schema name that was assigned to the administration database when the administration database was installed.

Authentication type
If you leave the default setting of Server, then the administration database user ID and password is sent to the administration database for validation.

If you click Client, no validation is performed by the database, and the user ID you type to log in to your system allows connection to the administration database. **Restriction:** when you log in to the client workstation, you must enter a user ID that has DB2 connect privileges.

Database connection ID
Type the user ID and password that was defined when the administration database was installed. The user ID and password must be locally defined on the server.

Enable single sign-on
Click True to enable single sign-on, if required by your EIP system plan.

FED Connector: Confirm Server Setup Information

This window displays the values you typed to configure the federated connector connectivity information.

Click **Next** to accept the values, or click **Back** to modify the values.

Configure system administration database

The installation program uses the information you enter on this window to connect to DB2, list the databases on the server and compare the name you define in the **Database name** field to existing databases on the server.

Tip: If you are sharing a Content Manager Version 8 database and want to verify the Content Manager Version 8 database name, or to avoid duplicating database names if you are installing a new EIP database, use DB2 Command Line Processor to list the databases on the server. At the prompt, type `LIST DATABASE DIRECTORY` at the `db2` prompt.

If the program detects a database with the same name, the program gives you the option to overwrite the database. If you are adding EIP tables to a Content Manager Version 8 database, do not overwrite the database. If the program does not detect an existing database with the same name, you are prompted to create a database. Follow the guidelines below when you define the information that identifies the administration database:

Database name

Type the administration database name. **Tip**: To avoid potential problems, do not use the special characters @, #, and $ in a database name if you intend to have a client remotely connect to a host database. Also, because these characters are not common to all keyboards, do not use them if you plan to use the database in another country. Unless otherwise specified, all names can include the following characters:

- A through Z. When used in most names, characters A through Z are converted from lowercase to uppercase.
- 0 through 9
- @, #, $, and _ (underscore)

Unless otherwise specified, all names must begin with one of the following characters:

- A through Z
- @, #, and $
- If you are installing an administration or Information Mining database, accept the default database name, or type the new name.
- If you are sharing a Content Manager Version 8 Library Server database, type the Content Manager Version 8 Library Server database name that was defined when the Library Server was installed.

Schema name

- If you are installing an administration or Information Mining database, you can accept the default name, which is the same name as the Database administration ID default user ID, or change the default schema name. Type the new database name in the Schema name field. The schema name can contain up to eight letters, can contain numerals, and will appear in capital letters.

- If you are sharing a Content Manager Version 8 database, type the Content Manager Version 8 Library Server database schema name that was defined when the Library Server was installed.

A schema is a collection of named objects. A schema also provides a logical classification of objects in the database. A schema can contain objects such as aliases, tables, views, indexes, triggers, distinct types, functions, and packages. A schema can be implicitly created when an object is created. The schema exists in the database as an object. If a schema name is not specified, the first eight letters of the authorization name of the creator of the object is used as the default.

Database administration ID

The user ID and password you define in this field is used only for database creation and must be locally defined and must have DB2 administration privileges. **Restriction:** You must log in to the server with a user ID that has DB2 administration privileges before you can create the administration database.

Database connection ID

The user ID and password you define in this field allows users to connect to the administration database. The user ID must be locally defined.

Database Already Exists

You see this window only if you have reused the name of an EIP database or you typed the name of a Content Manager Version 8 Library Server.

Replace the existing database?

If you click this option, DB2 drops the existing database and creates an EIP database. **Tip:** If you replace the existing database, the program prompts you twice for confirmation.

Select System Administration Server Options

You see this window only if you are installing an administration database that does not reuse the name of an existing administration database and you are not adding EIP tables to a Content Manager Version 8 database.

Enable unicode

Click True if you are installing Information Mining, or an administration database to which you plan to add Information Mining tables.

Enable text search

Click this box to enable text search.

Confirm System Administration Database Setup Information

This window displays the values you typed to define the administration database. Click **Next** to accept the values or **Back** to modify the values.

Image Search: Enter Client Setup Information

On this window, you define values that EIP uses to locate and connect to an image search server.

Image Search user ID
Type the name of the Image Search server that was defined when the server was installed.

Image Search Server name
Type the host name of the Image Search server. Ask the server administrator if you are required to enter a fully-qualified host name.

Host name
Type the host name that was defined when the Image Search server was installed.

Port number
Type the port number that was defined when the server was installed.

Control data path
Type the name of the Control data path for the Image Search client.

Image Search Client: Confirm Setup Information

This window displays the values defined for the Image Search client. Click **Next** to accept the values, click **Back** to modify the values.

Text Search: Enter Client Setup Information

On this window, you define values that EIP uses to locate and connect to a Text Search server.

Text Search Client user ID
Type the user ID required to connect to a text search server.

Text Search server name
Type the name of the Text Search server.

Text Search Host Name
Type the fully-qualified Text Search server host name.

Text Search Port number
Type the port number that was defined when the Text Search server was installed.

Text Search Client: Confirm Setup Information

This window displays the values defined for the Text Search client. Click **Next** to accept the values, click **Back** to modify the values.

Installation Status

This window displays the installation status of the components you selected. Click **Next** when the component installation is complete.

Specify RMI Host Name and Port Number

On this window, you define host name and port number for an RMI server and you can also define an RMI host name and port number for a workflow or Information Mining RMI server.

If your system plan includes a master RMI server, type the host name of the master server and the master server port number in the fields in the top half of this window. The default host name is the local server name, and the default port number is 1919. The RMI information is copied to `cmbclient.ini`. **Tip:** Ask the server administrator if you are required to enter a fully-qualified host name.

If your system plan includes a separate RMI server for workflow or Information Mining, type the host name and port number for the workflow or Information Mining RMI server in the fields in the bottom half of this window. This RMI information is copied to `cmbsvclient.ini`.

Tip: If your system plans include RMI, you must install and configure the connectors on the RMI server in a separate step before the clients can use the RMI server.

Installation Complete

Click **Finish** to complete installing EIP components on AIX. **Tip:** You are not required to restart the server.

Exporting classpath, environment variables on AIX

You must use a configuration program that exports classpath, environment variables and other information before you can use EIP.

1. cd to `/usr/lpp/cmb/bin`
2. Type `. ./cmbenv81.sh`

Verifying EIP installation on AIX

See Chapter 21, “Verifying a successful installation of Enterprise Information Portal on AIX”, on page 315.

Chapter 21. Verifying a successful installation of Enterprise Information Portal on AIX

Use information in this section to verify a successful installation of Enterprise Information Portal on an AIX system. It includes the following procedures:

- “Enterprise Information Portal First Steps”
- “Verify Enterprise Information Portal system administration database”
- “Verify system administration database and system administration client communication” on page 316
- “Verify Enterprise Information Portal connection to Content Manager Version 8” on page 318
- “Run low-level connection tests” on page 316

Enterprise Information Portal First Steps

The Enterprise Information Portal First Steps program allows you to load sample data into the Enterprise Information Portal system administration database. You perform the First Steps procedures differently depending whether you have all of your Enterprise Information Portal components installed on one system or if you have them installed on more than one system.

For an AIX installation of the system administration database, you need to run the First Steps program from the Windows system where you installed your system administration client component. See “Running First Steps with Enterprise Information Portal components installed on multiple machines” on page 196.

Verify Enterprise Information Portal system administration database

To verify that the Enterprise Information Portal system administration database is installed correctly:

__ 1. Check database connection by typing:

```
$ db2 connect to icmnlsdb user icmadmin using password
```

You should see output similar to the following:

```
Database Connection Information

Database server        = DB2/6000 7.2.4
SQL authorization ID   = ICMADMIN
Local database alias   = ICMNLSDB
```

__ 2. Check database tables by typing:

```
$ db2 list tables
```

You should see several tables listed (around 150); some with names starting with ″FA″ and some starting with ″ICM″.

Verify system administration database and system administration client communication

Because there is no administration client on AIX, you must configure a connection between the Windows administration client and the AIX databases. There are two ways to connect an administration client to a remote database.

- Connect through an RMI server (see Chapter 33, “Configuring an RMI server”, on page 507.
- Define a connection by following the steps in “Connecting the administration client to a remote administration database” on page 447.

Run low-level connection tests

Verify that the Enterprise Information Portal federated connector and the Content Manager Version 8 connector are installed correctly, run the indicated sample programs in this section.

Before you run the tests

Before you run the connection tests:

__ 1. It is important that any user ID that is used for EIP application development work must be a member of the group that your db2 instance user ID belongs to, for example: **db2iadm1** (the group that db2inst1 belongs to).

__ 2. Login as **icmadmin**. Perform the following setup to run the EIP sample programs. Copy the java samples to a local directory eipsamps off of your home directory:

```
 $  cp -R /usr/lpp/cmb/samples/java $HOME/eipsamps
```

This also changes the ownership of the files to the current user.

__ 3. Ensure you have the proper Enterprise Information Portal development environment. It is recommended that you add these two lines to the `.profile` of the users doing EIP application development work. Note the space between the period (.) and the first slash (/):

__ a. Establish the DB2 environment.

```
  $ . /home/db2inst1/sqllib/db2profile
```

__ b. Establish the EIP development environment.

```
$ . /usr/lpp/cmb/bin/cmbenv81.sh
```

Running the connection tests

Run the following two tests:

__ 1. **Federated connector test:**

```
$ cd $HOME/eipsamps/java/fed
$ javac TConnectFed.java
$ java TConnectFed icmnlsdb icmadmin password
```

Expected output:

```
$ java TConnectFed icmnlsdb icmadmin password
*** connecting to datastore : icmnlsdb
*** datastore connected ***
user icmadmin dsName icmnlsdb
datastore disconnected
user icmadmin dsName icmnlsdb
```

__ 2. **Content Manager V8 connector test:**

```
$  cd $HOME/eipsamps/java/icm
$  javac SConnectDisconnectICM.java
$  java SConnectDisconnectICM icmnlsdb icmadmin password
```

Expected output:

```
$ java SConnectDisconnectICM icmnlsdb icmadmin password
======================================
IBM Enterprise Information Portal v8
Sample Program:  SConnectDisconnectICM
--------------------------------------
Database: icmnlsdb
UserName: icmadmin
======================================
Connecting to datastore (Database 'icmnlsdb', UserName
         'icmadmin')...
Connected to datastore (Database 'icmnlsdb', UserName
         'icmadmin').
Disconnecting from datastore & destroying reference...
Disconnected from datastore & destroying reference.
==========================================
Sample program completed.
==========================================
```

If you get the following type errors:

```
TConnectFed.java:33: package com.ibm.mm.sdk.common does not
                                                  exist
import com.ibm.mm.sdk.common.*;
^
```

You forgot to establish the EIP development environment. Note the space between the period (.) and the first slash (/) in the command.

Execute:

```
$ . /usr/lpp/cmb/bin/cmbenv81.sh
```

Verify Enterprise Information Portal connection to Content Manager Version 8

To verify the connection from Enterprise Information Portal to Content Manager:

__ 1. On your Windows system, start the Enterprise Information Portal system administration client, as follows: Administration Client on Windows:

Start -> Programs -> Enterprise Information Portal V8.2 -> Administration

__ 2. On the left-hand side of the window, right-click on **Servers** and select **New**.

__ 3. From the list, select **Content Manager v8**.

__ 4. Enter the connection information:

Server Name: ICMNLSDB

__ 5. Click on the **Test Connection** button.

__ 6. You should see that the connection is successful.

Chapter 22. Installing the Content Manager eClient on AIX

After you have verified your Enterprise Information Portal installation, you can install the eClient.

If you are installing the eClient on the same machine that you installed Enterprise Information Portal, you do not need to install any additional prerequisites.

Before you install the eClient

Before you begin the installation process for the eClient, here are some things to consider:

If you are using WebSphere Application Server (WAS) AES, stop any server that is already running on WAS. However, if you are using WAS AE, make sure that the WebSphere Application Server administration server (AE) is running before starting the eClient installation.

If you are using WebSphere Application Server 5, make sure that you have started the application server. To start the application server:

1. Change to `WASROOT/bin` subdirectory, where *WASROOT* is the root directory where WebSphere is installed.
2. Execute

   ```
   ./startServer.sh server1
   ```

Installing the eClient

To install the eClient on your application server on AIX:

1. Insert the eClient CD into the CD drive.
2. **Optional:** If you are installing on AIX using an X window session (for example, Exceed), enter this command:

   ```
   export DISPLAY=hostname:0.0
   ```

   where `hostname` is the host name or IP address where you want to be able to view the install panels.
3. From the launchpad directory, enter this Java command to manually run the launchpad:

   ```
   java com.ibm.cm.install.launchpad.LaunchPad
   ```

   Note: You must have root or sudo privileges to run the launchpad.

4. Follow the instructions in the installation windows. The default directory to install the eClient is `/opt/CMeClient`.
5. If you are connecting to Content Manager Version 8, the default local file location of the data server list file is `/usr/lpp/cmb/cmgmt/cmbicmsrvs.ini`

   After you install the eClient files, the installation program checks for WebSphere Application Server (WAS). If the installation program detects WAS, you can continue with the automatic configuration of the Web application for the eClient. You can choose to exit without automatically configuring the application with WebSphere.
6. Start the eClient on WebSphere. To start the eClient on WebSphere:
   a. Change to the `/Save` subdirectory.
   b. For WebSphere 4.0.5 AE, enter `startIDMAE.sh`; for WebSphere 4.0.5 AES, enter `startIDMAES.sh`; for WebSphere 5, enter `startIDMServer.sh`.

   To stop the eClient, enter `stopIDMAE.sh` or `stopIDMAES.sh`.
7. **Optional:** If you choose not to perform the automatic configuration, you must set up and configure the eClient as a Web application.

Validating the eClient installation

Follow these steps to validate that the eClient is installed correctly:

For WebSphere AES

__ 1. After installation has completed, if you are using WebSphere AES, you need to start the server:

```
$ /usr/WebSphere/AppServer/bin/startServer.sh
```

__ 2. Execute the utility to start the eClient in WebSphere:

```
/opt/CMeClient/Save/startIDMAES.sh
```

__ 3. Before starting the eClient, start the WebSphere Admin console to confirm that the eClient Application Server has been created. Start it if necessary.

__ 4. In your browser, enter:

```
http://<hostname>/eClient82/IDMInit
```

The eClient login page should open.

For WebSphere AE and WebSphere Version 5

__ 1. Execute the utility to start the eClient in WebSphere:

```
/opt/CMeClient/Save/startIDMAE.sh
```

__ 2. Before starting the eClient, start the WebSphere Admin console to confirm that the eClient Application Server has been created. Start it if necessary.

__ 3. In your browser, enter:

```
http://<hostname>/eClient82/IDMInit
```

The eClient login page should open.

If you installed the eClient correctly and the address is correct, the Logon window should open.

If you configured the eClient correctly, you should be able to access the content servers that you defined. The content servers that the eClient supports include:

- IBM Content Manager for Multiplatforms Version 7.1
- IBM Content Manager for Multiplatforms Version 8.1
- IBM Content Manager for Multiplatforms Version 8.2
- IBM Content Manager OnDemand for Multiplatforms Version 7.1
- IBM Content Manager OnDemand for OS/390 Version 2.1
- IBM Content Manager OnDemand for OS/390 Version 7.1
- IBM Content Manager OnDemand for iSeries Version 4.5
- IBM Content Manager OnDemand for iSeries Version 5.1
- IBM Content Manager ImagePlus for OS/390 Version 3.1
- IBM VisualInfo for AS/400 Version 4.3 or Version 5.1

Part 4. Installing Content Manager on a Sun Solaris operating system

This section contains information needed to install and configure the IBM Content Manager and Enterprise Information Portal software on the Solaris operating system. The information in this section is based on the steps identified using the *Planning Assistant* from the *Start Here CD*.

The prerequisite and installation details in this section are presented in the required order of installation. All steps are presented as if each one is required on this single workstation (for a single server configuration). In fact, you may only need some of the steps, depending on your own configuration needs:

1. Chapter 23, "Installing and updating prerequisite programs on Solaris", on page 325
2. Chapter 24, "Performing pre-installation steps on Solaris", on page 345
3. Chapter 25, "Installing Content Manager components on Solaris", on page 355
4. Chapter 26, "Verifying a successful installation of Content Manager on Solaris", on page 393
5. Chapter 27, "Installing Enterprise Information Portal components on Solaris", on page 417
6. Chapter 28, "Verifying a successful installation of Enterprise Information Portal on Solaris", on page 421
7. Chapter 29, "Installing Content Manager eClient on Solaris", on page 425

Chapter 23. Installing and updating prerequisite programs on Solaris

This section has two sub-sections:

__ 1. "Verifying your software Prerequisites on Solaris" explains how to check the level of a prerequisite that you already have installed on your system.

__ 2. "Installing / Updating Prerequisites" on page 327 has detailed instructions for how to install and configure the prerequisite programs that are needed for your own planned configuration.

- The steps that you need to perform are determined by the selections that you make while you are using the ″Planning Assistant″ from the *Start Here CD*.
- The planning assistant produces output sheets (with checklists) for the programs and components that you need to install for your selected components.

The prerequisite programs included in this section are:

- "Patch for Solaris 8 operating environment" on page 327
- "Sun Forte C++ Compiler Version 6.1" on page 327
- "IBM DB2 Universal Database" on page 328
- "Oracle database on a Solaris system" on page 335
- "IBM DB2 Net Search Extender (NSE) and Text Information Extender (TIE)" on page 338
- "IBM WebSphere Application Server (WAS)" on page 339

Verifying your software Prerequisites on Solaris

Run the following verification checks to determine which of the prerequisites you need to install or update. For those prerequisites that are either not installed or at the expected level, use the next section to guide you through installing them.

Table 118. Basic prerequisites

Prerequisite	How to check	Expected value
Solaris version 2.8	`uname -r`	level#: 5.8
Solaris patch 108528	`showrev	grep version`	level#: 108528-08 or higher
Sun Forte C++ compiler	`pkginfo -l SPROvws	grep VERSION`	level#: 6.1or higher

Table 118. Basic prerequisites (continued)

Prerequisite	How to check	Expected value

DB2 UDB V8.1	`pkginfo -l  db2engn71 | grep VERSION`
	`pkginfo -l  db2engn81 | grep VERSION`
		level#: 8.1.1.0

DB2 UDB Enterprise Server Edition Version 8.1 with Fixpack 1	From the DB2 Command Window: `db2level`	Level needs to read SQL08010 or read ″DB2 v8.1.1.27″. The fixpack information needs to read ″FixPak ″1″ and list the fixpack level, for example, ″s021124″ is the fixpack that had been available November 24,2002. For Oracle, the fixpack level must be S021110 or later.
DB2 Text Information Extender v7.2	`pkginfo -l  db2tie72 | grep VERSION`	level#: 7.2.0.0

Net Search Extender (required if you use DB2 Version 8.1)	From the DB2 Command Window, start the text search program:
	`db2text start`
	Then type:
	`db2textlevel`
		CTE0350 Instance ″DB2″ uses DB2 Net Search Extender code release ″ tx9_81″ with level identifier ″ tx9_26a″

Tivoli Storage Manager API Client Version 4.2.1	`/opt/tivoli/tsm/client/api/samprun` Where `opt` is the install directory	API Library Version = 4.2.1.0
Tivoli Storage Manager Server Version 4.2.1	Logon to the TSM Server Administration Web page: `http://<hostname>:1580` Where `<hostname>` is the name of the TSM server.	The version appears on the Web page. It should say Version 4, Release2, Level1.0
WebSphere AppServer AES or WebSphere AppServer AE	`grep /version /opt/WebSphere/AppServer /properties/com/ibm /websphere/product.xml`	<version>4.0.3 </version>

Table 119. Additional prerequisites for Oracle

Prerequisite	How to check	Expected value
DB2 Relational Connect Version 8.1 with fixpack1	From a DB2 Command Window: `db2level`	Level: s021110 or later
Oracle Version 8.1.7.4 or Version 9.2.0.1	Connect to an existing Oracle database: `Sqlplus userID/user_password@ databasename.domainname`	Oracle 8i Enterprise Edition 8.1.7.4.0 PL/SQL 8.1.7.4.0 TNS for 32-bit Windows: 8.1.7.4.0
	To check the version type: `select * from product_component_version;`	Oracle 9i Enterprise Edition 9.2.0.1 PL/SQL 9.2.0.1 TNS for 32-bit Windows: 9.2.0.1

Installing / Updating Prerequisites

The following sections guide you through installing each of the prerequisites including fixpacks, how to install them, and how to verify them after installation.

The rule of thumb when installing the prerequisites is to always apply the fixpacks after your base components are installed. For instance if you are missing the DB2 UDB Application Development Client from your DB2 install, install this component first, then install the fixpack code. Otherwise you will need to install the fixpack code again after adding any new DB2 components.

Patch for Solaris 8 operating environment

You need to have Solaris Version 2.8 installed on your system. Assuming that you do, you can use the SunSolve Online website to download the required patch (108528). Follow the download and installation instructions provided at the SunSolve download site:

http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access

To validate the patch installation, rerun the `showrev` command:

```
showrev | grep version
```

You should see the following output:

```
108528-08 (or later)
```

Sun Forte C++ Compiler Version 6.1

You should have Forte C++ compiler available on the system. You can use the following command to verify that you do:

```
pkginfo -l  SPROvws | grep VERSION
```

If Forte C++ compiler is installed, you see the following output:

```
VERSION: 6.1
```

IBM DB2 Universal Database

IBM DB2 Universal Database Enterprise Edition Version 7.2 OR Enterprise Extended Edition Version 7.2.1. (or higher) is required for Content Manager Version 8 Release 2 servers when you use DB2 for your server databases. IBM DB2 Universal Database Enterprise Server Edition Version 8.1 is required when you use Oracle for your server databases. IBM DB2 Universal Database Enterprise Server Edition Version 8.1 (at fixpack 1 code level) is included in the Content Manager package.

If you are planning to use a DB2 database for your library server and resource manager, continue with this section to install IBM DB2 Universal Database Enterprise Server Edition Version 8.1 (included in the Content Manager package).

If you are planning to use an Oracle database with your Content Manager library server and resource manager, use the instructions for installing DB2 Universal Database and DB2 Relational Connect that are provided in the section: “Oracle database on a Solaris system” on page 335.

Before you begin to install IBM DB2 Universal Database

Before you begin to install IBM DB2 Universal Database, complete the following steps:

__ 1. Ensure that your machine has enough memory and disk space for your installation. See the DB2 product documentation on the DB2 Online Support Web site for the requirements at:

www.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8pubs.d2w/en_main

__ 2. Make sure that you do not have a previous version of DB2 already installed on the machine. If a previous version of DB2 is installed, you need to migrate servers and instances, depending on the version installed. In this case, do not follow these instructions. Instead, refer to the DB2 product documentation on the DB2 Online Support Web site at:

www.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8pubs.d2w/en_main

__ 3. Your DB2 database server will reside on the same machine as WebSphere Application Server. This configuration and the use of the default settings documented in these instructions are appropriate only for development and small production environments. For larger environments where it is preferable to configure the DB2 server on a remote machine, you must install and configure a DB2 client on the same machine on which you install WebSphere Application Server and verify the remote database connectivity. See the IBM Redbook, *WebSphere V3.5 Handbook*, on the IBM Redbooks Web site at:

www.redbooks.ibm.com/redbooks/SG246161.html

for more information about implementing this configuration.

Important: Install DB2 before installing WebSphere Application Server.

__ 4. The DB2 CD in the package may contain a compressed image. You may have to untar it before you use it.

Installing IBM DB2 Universal Database

Perform the following steps to install DB2:

__ 1. Ensure that you are logged into the machine with super user (root) privileges.

__ 2. Ensure that you have set the following UNIX kernel, shared memory, and semaphore parameters properly:

```
MSGMAX
MSGMNB
MSGMAP
MSGMNI
MSGSSZ
MSGTQL
MSGSEG
SHMMAX
SHMSEG
SHMMNI
SEMMNI
SEMMAP
SEMMNS
SEMMNU
SEMUME
```

Refer to the *DB2 Quick Beginnings for UNIX* and related DB2 UDB documentation (to obtain information on the proper values for these parameters) on the DB2 Online Support Web site at:

www.ibm.com/cgi-bin/db2www/data/db2/udb
/winos2unix/support/v8pubs.d2w/en_main

It is recommended that you review these settings with your system administrator to ensure that they do not conflict with settings necessary for other software programs on your system. You can use the following sample files to update the settings for these parameters. The files are located in the `/db2/install/samples` directory on the DB2 software CD-ROM or in the `/opt/IBMdb2/V8.1/cfg` directory in the installed DB2 product:

```
kernel.param.64MB for systems with 64 - 128 MB physical memory
kernel.param.128MB for systems with 128 - 256 MB physical memory
kernel.param.256MB for systems with 256 - 512 MB physical memory
kernel.param.512MB for systems with 512 MB to 1 GB physical memory
```

__ a. Choose the file appropriate for your system

__ b. Append it to the /etc/system file

__ c. Make any changes to the SHMMAX parameter if needed (as outlined in the DB2 product documentation)

__ d. Enter the command

```
# touch /reconfigure
```

__ e. Restart your machine.

__ 3. Insert the DB2 UDB CD-ROM, and if necessary, mount the CD-ROM drive.

Hint: On most Solaris systems, the Volume Management daemon (**vold**) mounts the CD-ROM automatically and immediately, as well as each time the machine is restarted. If the **vold** process is not running on the local machine, see your Solaris system documentation for instructions on how to mount the CD-ROM drive.

The following steps assume that the CD-ROM drive is mounted at /cdrom.

__ 4. Navigate to the correct directory on the DB2 UDB CD-ROM by entering the following command:

```
# cd /cdrom/cdrom0
```

__ 5. Enter the following command to start the DB2 installation using the DB Setup Utility:

```
 # ./db2setup
```

Important: The DB2 Setup Utility works with only the bash, Bourne, and Korn shells.

__ 6. From the IBM DB2 Setup Launchpad (Welcome) window, you can view installation prerequisites and the release notes. You may want to review the installation prerequisites and release notes for late-breaking information. Click **Install Products** to begin the installation.

__ 7. The Setup window opens. Select DB2 UDB Enterprise ServerEdition, then click **Next**.

__ 8. Once you have initiated the installation, proceed by following the setup program’s prompts.

When prompted, select **Typical** as the installation type, to install all DB2 components required to support Content Manager. You can take most default options (unless you have specific requirements of your own).

Online help is available to guide you through the remaining steps. To invoke the online help, click **Help** or press **F1**. You can click **Cancel** at any time to end the installation. DB2 files will only be copied to your computer once you have clicked **Finish** on the last DB2 Setup wizard installation panel.

__ 9. Unmount the CD-ROM before removing it from the CD-ROM drive by entering the following command:

```
# umount cdrom/cdrom0
```

Steps to complete after installing DB2 and before installing Content Manager

After you install DB2, perform the following steps for Content Manager:

__ 1. Ensure that you are logged into the machine with super user (root) privileges.

__ 2. Create home directories for the DB2 Instance, DB2 Fenced User, and DB2 Administration Server. These directory names must match the values for the Home Directory option that you designate when configuring the DB2 Instance, DB2 Fenced User, and DB2 Administration Server in the procedures listed under Steps 7, 8 on page 332, and 12 on page 332.

__ 3. Navigate to the directory containing the DB2 Setup Utility by entering the following command:

```
# cd /opt/IBMdb2/V8.1/install
```

__ 4. Start the DB2 Setup Utility by entering the following command:

```
# ./db2setup
```

__ 5. Highlight the **Create** button beside the option labeled **To create a DB2 Instance, an Administration Server, or a Data Links Manager Administrator**, select **Create** and press **Return**.

__ 6. In the Create DB2 Services window, highlight the **Create a DB2 Instance option** and press **Return**.

__ 7. In the DB2 Instance window, perform the following steps, noting the values that you enter or accept for future reference:

  __ a. Enter a user name or accept the default value for the **User Name** option. You will specify this user name when you configure WebSphere Application Server.

  __ b. Enter a user ID or accept the default user ID by ensuring that the **Use default UID** option has an asterisk (*) beside it.

  __ c. Enter a group name or accept the default value for the Group Name option.

  __ d. Enter a group ID or accept the default group ID by ensuring that the **Use default GID** option has an asterisk (*) beside it.

__ e. Enter a home directory or accept the default value for the Home Directory option. You will specify this directory when you configure WebSphere Application Server.

__ f. Type a password for the user in the **Password** and **Verify Password** options. DB2 requires a password of eight or fewer characters. You will specify this password when you configure WebSphere Application Server.

__ g. Highlight **OK** and press **Return**.

__ 8. In the Fenced User window, perform the following steps, noting the values that you enter or accept for future reference:

__ a. Enter a user name or accept the default value for the **User Name** option.

__ b. Enter a user ID or accept the default user ID by ensuring that the **Use default UID** option has an asterisk (*) beside it.

__ c. Enter a group name or accept the default value for the **Group Name** option.

__ d. Enter a group ID or accept the default group ID by ensuring that the **Use default GID** option has an asterisk (*) beside it.

__ e. Enter a home directory or accept the default value for the **Home Directory** option.

__ f. Type a password for the user in the **Password** and **Verify Password** options. DB2 requires a password of eight or fewer characters.

__ g. Highlight **OK** and press **Return**.

__ 9. In the DB2 Warehouse Control Database window, highlight the option labeled **Do not set up DB2 Warehouse Control Database** and press **Return**.

__ 10. Highlight **OK** and press **Return**.

__ 11. In the Create DB2 Services window, highlight the **Create the Administration Server** option and press **Return**.

__ 12. In the Administration Server window, perform the following steps, noting the values that you enter or accept for future reference:

__ a. Enter a user name or accept the default value for the **User Name** option.

__ b. Enter a user ID or accept the default user ID by ensuring that the **Use default UID** option has an asterisk (*) beside it.

__ c. Enter a group name or accept the default value for the **Group Name** option.

__ d. Enter a group ID or accept the default group ID by ensuring that the **Use default GID** option has an asterisk (*) beside it.

__ e. Enter a home directory or accept the default value for the **Home Directory** option.

__ f. Type a password for the user in the **Password** and **Verify Password** options. DB2 requires a password of eight or fewer characters.

__ g. Highlight **OK** and press **Return**.

__ 13. A notice window informs you of the value being created for the DB2SYSTEM environment variable. Ensure that **OK** is highlighted and press **Return**.

__ 14. In the Create DB2 Services window, highlight **OK** and press **Return**.

__ 15. The Summary Report window shows the choices you have made so far. When you have determined that the information is correct, ensure that **Continue** is highlighted and press **Return**.

__ 16. A warning window opens, giving you the option of canceling the processes. Ensure that **OK** is highlighted and press **Return**.

__ 17. A notice window informs you when the processes are completed. Ensure that **OK** is highlighted and press **Return**.

__ 18. The Status Report window informs you of process successes and failures. View the Log File for information on how to correct particular failures. To exit from this window, ensure that **OK** is highlighted and press **Return**.

__ 19. In the DB2 Setup Utility window, highlight **Close** and press **Return**.

__ 20. In the notice window, ensure that **OK** is highlighted and press **Return**.

__ 21. Make the root user a member of the administrative group that you accepted or designated for the **Group Name** option during the creation of the Administrative Server by editing the `/etc/group` file.

__ 22. If you are developing or running applications and want to avoid specifying the full path to the product libraries and include files, consider creating symbolic links. Create symbolic links for the DB2 files to the /usr/lib directory and for the include files to the /usr/include directory by entering the following command:

```
# /opt/IBMdb2/V8.1/cfg/db2ln
```

__ 23. Configure the root user to run the **db2profile** script at login by adding the following line to the `.profile` or `.dtprofile` file for the user root (assuming that the user root uses the Korn or Bourne shell and that `/export/home/db2inst1` is the home directory of the example instance owner db2inst1):

```
. /export/home/db2inst1/sqllib/db2profile
```

This action is required to install and run WebSphere Application Server. If the user root uses a shell other than the Korn shell or Bourne shell, make appropriate changes to this information.

__ 24. Log out and then log back in for your changes to take effect.

Validating the IBM DB2 Universal Database installation

To demonstrate that DB2 is functioning correctly, you can create a sample database and compile and execute a Java application that accesses it. You can see that the environment is set up correctly for DB2 and for IBM Java 2 SDK, and that the JDBC provider is accessible from a Java application.

Perform the following steps to create the sample database and compile and run the Java application:

__ 1. Ensure that you are logged in as the DB2 instance owner, **db2inst1**.

__ 2. Ensure that the DB2 environment has been set up correctly by using the echo command to verify the value of the `DB2INSTANCE` environment variable, as follows:

```
 $ echo $DB2INSTANCE
```

The correct value returned is **db2inst1**.

__ 3. Ensure that the home directory of the instance owner, `/export/home/db2inst1`, has write permissions.

__ 4. Create the sample database by executing the db2sampl script, as follows:

```
$ db2sampl
```

This process can take several minutes to complete.

__ 5. Ensure that you are in the instance owner's home directory, `/export/home/db2inst1`.

__ 6. Compile an example Java application by using the javac command, as follows:

```
$ javac -d . sqllib/samples/java/DB2Appl.java
```

The resulting class file is created in the local directory.

__ 7. Start DB2 by using the db2start command, as follows:

```
$ db2start
```

__ 8. Run the Java sample by using the **java** command, as follows:

```
$ java DB2Appl
```

Correct output resembles the following:

```
Retrieve some data from the database...
Received results:
empno= 000010 firstname= CHRISTINE
empno= 000020 firstname= MICHAEL
```

```
empno= 000030 firstname= SALLY
. . .
Update the database...
Changed 1 row.
```

Oracle database on a Solaris system

This section helps you set up the required prerequisite programs if you want to access Oracle data sources for your library server. Depending on your planned configuration, you will be installing the following software:

For the library server database component

- Oracle Enterprise server software, Version 8.1.7.4 OR Version 9.2.0.1 or later
- IBM DB2 Universal Database Enterprise Server Edition Version 8.1 with fixpack 1 applied (s021110 or later)
- DB2 Relational Connect Version 8.1 with fixpack 1 applied (s021110 or later)

For the library server application component

If the library server application component is going to be installed on the same machine as the library server database component:

- Oracle Enterprise server software, Version 8.1.7.4 OR Version 9.2.0.1 or later
- IBM DB2 Universal Database Enterprise Server Edition Version 8.1 with fixpack 1 applied (s021110 or later)
- DB2 Relational Connect Version 8.1 with fixpack 1 applied (s021110 or later)

If the library server database component is going to be installed on a remote Oracle server machine from the library server application component:

- Oracle Enterprise client software, Version 8.1.7.4 OR Version 9.2.0.1 or later

Before you begin to install the Oracle server or client software

Before you begin to install IBM DB2 Universal Database, ensure that your machine has enough memory and disk space for the installation, and that you meet all the requirements for the installation. See the following Oracle web site for the platform-specific requirements:

http://technet.oracle.com

Installing the Oracle server software for the library server database component

To install Oracle Enterprise Edition server software, Version 8.1.7.4 OR Version 9.2.0.1 (or later):

__ 1. Log on to the system as a user ID that has root authority.

__ 2. Use the installation procedures in the documentation that comes with the Oracle software for details on how to install the Oracle server software.

Installing the Oracle client software for a remote library server application component

To install Oracle Enterprise Edition client software, Version 8.1.7.4 OR Version 9.2.0.1 (or later):

__ 1. Log on to the system as a user ID that has root authority.

__ 2. Use the installation procedures in the documentation that comes with the Oracle software for details on how to install the Oracle client software. Become aware of any compatibility issues between different levels of Oracle client software and Oracle server software by consulting Oracle documentation, the Oracle TechNet website, the Oracle Metalink website, or Oracle customer service.

__ 3. To ensure that the client software is able to connect to the Oracle server, use the Oracle **sqlplus** tool to connect to an existing database on the Oracle server.

You should see the following fields in your `sqlnet.ora` file in your `ORACLE_HOME/NETWORK/ADMIN` directory:

```
SQLNET.AUTHENTICATION_SERVICES=(NTS)
NAMES.DIRECTORY_PATH= (TSNAMES,ONAMES,HOSTNAME)
```

Before you begin to install IBM DB2 Universal Database

Before you begin to install IBM DB2 Universal Database, complete the following steps:

__ 1. Ensure that your machine has enough memory and disk space for your installation. See the DB2 product documentation on the DB2 Online Support Web site for the requirements at:

> www.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8pubs.d2w/en_main

__ 2. Make sure that you do not have a previous version of DB2 already installed on the machine. If a previous version of DB2 is installed, you need to migrate servers and instances, depending on the version installed. In this case, do not follow these instructions. Instead, refer to the DB2 product documentation on the DB2 Online Support Web site at:

> www.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8pubs.d2w/en_main

__ 3. Your DB2 database server will reside on the same machine as WebSphere Application Server. This configuration and the use of the default settings documented in these instructions are appropriate only for development and small production environments. For larger environments where it is preferable to configure the DB2 server on a remote machine, you must install and configure a DB2 client on the same machine on which you install WebSphere Application Server and verify the remote database connectivity. See the IBM Redbook, *WebSphere V3.5 Handbook*, on the IBM Redbooks Web site at:

www.redbooks.ibm.com/redbooks/SG246161.html

for more information about implementing this configuration.

Important: Install DB2 before installing WebSphere Application Server.

__ 4. The DB2 CD in the package may contain a compressed image for DB2 ESE and for DB2 Relational Connect. Your may have to untar it before you use it.

Installing IBM DB2 Universal Database Enterprise Server Edition

To Install IBM DB2 Enterprise Server Edition:

__ 1. Insert and mount the DB2 CD into the CD-ROM. Change to the directory where the CD-ROM is mounted. Enter the **./db2setup** command to start the DB2 Setup Wizard.

__ 2. From the IBM DB2 Setup Launchpad (Welcome) window, you can view installation prerequisites and the release notes. You may want to review the installation prerequisites and release notes for late-breaking information. Click **Install Products** to begin the installation.

__ 3. Proceed through the DB2 Setup Wizard installation panels and make your selections.

Note: As part of the installation, do not create a DB2 instance. You will create the instance when you install DB2 Relational Connect.

Installation help is available to guide you through the steps. To invoke the installation help, click Help or press F1. You can click Cancel at any time to end the installation.

__ 4. Click Finish on the last DB2 Setup Wizard installation panel to copy the DB2 files to your system.

When you complete the installation, DB2 is installed in the following directory:

```
/opt/IBM/db2/V8.1
```

Installing IBM DB2 Universal Database Relational Connect

After you install the client software and the DB2 server software, you need to install DB2 Relational Connect, Version 8 on the DB2 server. DB2 Relational Connect contains the software that you need to access Oracle data sources.

__ 1. Log on to the system under a user ID that has root authority.

__ 2. Close all open programs so that the installation program can update files as required.

__ 3. Insert the DB2 Relational Connect CD, and start the setup program to install DB2 Relational Connect.

- Insert and mount the DB2 Relational Connect CD into the CD-ROM. Change to the directory where the CD-ROM is mounted. Enter the ./db2setup command to start the setup program.

__ 4. The DB2 Relational Connect Setup Launchpad opens. From this window review the installation prerequisites and release notes for late-breaking setup information.

__ 5. From the Select the features to install panel in the setup program, choose **Relational Connect for Oracle Data Sources**. The set up will require you to identify the local path where you installed the Oracle client software.

The Relational Connect installation will update the `sqllib/cfg/db2dj.ini` file to set the ORACLE_HOME environment variable. If you need to set the ORACLE_BASE and ORA_NLS environment variables, you will need to set them manually.

The installation will also link DB2 to the Oracle client software.

Caution: If you do not install the Oracle client software before you run the DB2 Relational Connect installation, you will have to manually set the environment variables and link DB2 to the client software.

Installation help is available to guide you through the steps. To invoke the installation help, click Help or press F1. You can click Cancel at any time to end the installation.

__ 6. As part of the installation:

- Create a DB2 instance on the federated server. This will set the DB2 database manager FEDERATED parameter to YES, which enables the DB2 server to access the data sources.
- Specify the user authorities information for the instance.

__ 7. Click **Finish** on the last setup installation panel to copy the DB2 Relational Connect files to your system.

When you complete the installation, DB2 Relational Connect is installed in the same directory as the DB2 server software.

After the software is installed, a user with SYSADM authority should check the setup and create the federated database. The DB2 instance owner then configures the server to access the Oracle data sources.

IBM DB2 Net Search Extender (NSE) and Text Information Extender (TIE)

The powerful text search capabilities of the DB2 Version 7 Text Information Extender (TIE) are merged into the Net Search Extender (NSE) Version 8. Notice that if you plan to use the (optional) text search feature of Content Manager, you must install:

IBM Text Information Extender (TIE), Version 7.2 with IBM DB2 Enterprise Edition Version 7.2 and Enterprise Extended Edition Version 7.2.1

OR

IBM Net Search Extender (NSE), Version 8 with IBM DB2 Enterprise Server Edition, Version 8.1.

If you are using Oracle as your database application with Content Manager, AND you plan to use the (optional) text search feature of Content Manager, you must install NSE and not TIE.

IBM Net Search Extender (NSE), Version 8 is provided in the package with Content Manager, Version 8.2.

Installing IBM DB2 NSE

Refer to the installation instructions on the documentation CD supplied with DB2 Net Search Extender (NSE).

NSE must be installed on the same workstation as the library server.

Validating the DB2 NSE installation

To verify proper NSE installation, make sure DB2 is started and execute the following command to start DB2 NSE:

```
db2text start
```

You should see the following output:

```
 CTE0001 Operation completed successfully.
```

IBM WebSphere Application Server (WAS)

Installing IBM WebSphere Application Server

Use this section to install IBM WebSphere Application Server:

__ 1. Go to the WebSphere 5.0 InfoCenter online documentation for your configuration of the Application Server and in your language at:

http://www.ibm.com/software/webservers/appserv/infocenter.html

__ 2. Under the section entitled ″Version 5 InfoCenters:″, select your language in the drop-down box next to **Application Server for distributed operating systems**.

__ 3. Expand **Getting Started -> Installing WebSphere Application Server -> Installing the product** in the left navigation panel of the WebSphere InfoCenter

__ 4. Follow the instructions in the right panel for installing WebSphere as it applies to your operating system.

Validate the installation

To validate the WebSphere installation, use the information under **Getting Started -> Installing WebSphere Application Server -> Using the installation verification steps** in the WebSphere InfoCenter (that you opened during the installation steps above).

Installing MQSeries Workflow on Solaris

Prerequisites

- Solaris Version 2.8 or later
- IBM WebSphere MQSeries for Solaris Version 5.3.0.1 or higher
- IBM DB2 Universal Database for AIX Version 7.2 or higher.

Creating users and groups

1. Log on as root.
2. Enter command: groupadd fmcgrp
3. Verify that MQSeries Administrator group mqm exists
4. Verify that DB2 database administrator group db2iadm1 exists.

   If it does not exist, check to see that you have installed DB2 correctly. If your DB2 Administrator group has a different name, be careful to substitute it whenever the default db2iadm1 is mentioned.
5. Follow these steps to create an MQ Workflow Administration user. Note that the MQ Workflow Administration user ID (for example, fmc) must have MQSeries and DB2 administration rights. Use the following command to create the user. The following example assumes the db2 instance is of the db2iadm1 group.

   ```
   useradd -g fmcgrp -G mqm,db2iadm1 -d /export/home
         /fmc -s /usr/bin/ksh -m fmc
   ```
6. Set the password for user fmc with the command: passwd fmc
7. Modify fmc's login file to include locale information. For example:

   ```
   export LANG=en_US
   ```

   MQSeries Workflow runtime needs that locale information to look up message bundles.
8. Establish the use of db2 environment in fmc's profile. You can achieve this by in the fmc's profile including the db2profile of the db2 instance which owns the MQSeries Workflow runtime database. For example, include the following in the fmc's profile. The example assumes the db2inst1 is the instance owner and db2inst1 is used for the MQSeries Workflow runtime database.

   ```
   export DB2INSTANCE=db2inst1
   ```

   ```
   if [ -e /home/$DB2INSTANCE/sqllib/db2profile ];
   then    . /home/$DB2INSTANCE/sqllib/db2profile fi
   ```

Installing MQ Workflow on Solaris

The MQSeries Workflow runtime data will use /var/fmc by default. Depend on usage, it would take about 100MB to 400MB of disk space. It is recommended to check to see if the system has sufficient disk space before the installation is attempted.

1. Log on to the Solaris system as root.
2. Insert the MQ Workflow installation disk into the CD-Rom drive.
3. Copy all the files in the WFInstall directory from the CD-Rom to a temporary directory (for example, `/tmp/WFInstall`).
4. Specify the locale for this install as well as the following configuration session. For example: export `LANG=en_US`
5. Use the CMBWFSUNInstall.sh to install the MQSeries Workflow. For example: `CMBWFSUNInstall.sh /cdrom/fmc-3.4.0.pkg` **Restriction:** You can not use admintool to install the MQSeries Workflow for Solaris.

Important: The following kernel configuration parameters information is taken from the MQSeries Workflow 3.3 manual. Check the MQSeries Workflow 3.4 to see if there is additional recommendation update that you could use.

Kernel configuration parameters

There are recommended values for the Sun Solaris kernel configuration parameters. This summarizes the requirements from the *IBM DB2 Connect:Quick Beginning*s, and *MQSeries for Sun Solaris: Quick Beginnings* manuals:

- set msgsys:msginfo_msgmax = 65535
- set msgsys:msginfo_msgmnb = 65535
- set msgsys:msginfo_msgmap = 1026
- set msgsys:msginfo_msgmni = 256
- set msgsys:msginfo_msgssz = 16
- set msgsys:msginfo_msgtql = 1024
- set msgsys:msginfo_msgseg = 32767
- set shmsys:shminfo_shmmax = 483183820 (90% of your physical memory)
- set shmsys:shminfo_shmseg = 1024
- et shmsys:shminfo_shmmni = 1024
- set shmsys:shminfo_shmmin = 1
- set semsys:seminfo_semaem = 16384
- set semsys:seminfo_semvmx = 32767
- set semsys:seminfo_semmni = 1024 (semmni < semmns)
- set semsys:seminfo_semmap = 1026 (semmni + 2)
- et semsys:seminfo_semmns = 16384

- set semsys:seminfo_semmsl = 100 set semsys:seminfo_semopm = 100
- set semsys:seminfo_semmnu = 2048
- set semsys:seminfo_semume = 256
- set maxusers = 32 (This is the minimum, best to set it higher)

Note: The default for maxusers is the size of main memory in MB minus 2. For example, if you have 512 MB memory, maxusers defaults to 510. You can omit the set maxusers command from the /etc/system file.

Configuring MQWorkflow on Solaris

1. While still log on as root, find the CMBWFConfig.SUN.dat file and open it for editing.
2. Update the MQCommunicationAddress entry to replace the localhost with your machine name or IP address. For example:

   ```
   MQCommunicationAddress=hayes.svl.ibm.com
   ```
3. If the fmc is not using db2inst1, update the following entries to reflect the proper db2 instance owner.

   `RTDB2Instance`, `RTDB2LocalInstance`, `RTDatabaseContainerDirectory`, `RTDatabaseLocation`, `RTDatabaseLogLocation`
4. The default queue manager for the MQ Workflow is listening to port 5010. Check the `/etc/services` to see if it is being taken. Update the MQPort entry in the file to a different number if it's needed.
5. Save the edited `CMBWFConfig.SUN.dat` file.
6. Make sure to allow the fmc user to be able to read and run those EIP configuration files as well as write configuration log file into this directory.
7. Make sure there is no errors in the fmc user's .profile as the configuration script will `su` to `fmc`.
8. Run the `CMBWFSUNConfig.sh` under `root`. You will be prompted to enter `fmc`'s password. This script will create the MQSeries Workflow FMC configuration, create the MQSeries Workflow runtime database FMCDB, create the FMCQM queue manager, create the EIP workflow queue, and define the EIP workflow container data structures.

   Tips: Find the MQSeries Workflow manual references to these MQSeries Workflow utilities: fmczkcfg and fmczutil for usage details on how to customize your MQSeries Workflow configuration. Note that the EIP is default to work with only MQSeries Workflow FMC configuration and FMCQM queue manager. Do not change these settings in your MQSeries Workflow configuration.
9. Type dspmq. You should be able to see the FMCQM queue manager registered on the system. For example:

   ```
   QMNAME(FMCQM)                                     STATUS(Ended normally)
   ```

10. Type `fmczkcfg -o=l`. You should be able to see the MQSeries Workflow FMC configuration registered on the system. For example:
    - `FMC33611I The following configurations are defined: FMC`

The customization of MQSeries Workflow for the EIP workflow is now completed.

Starting EIP workflow on Solaris

EIP Advanced workflow uses MQSeries Workflow as the underlying workflow engine to deliver workflow functionality. Therefore, starting EIP workflow includes steps to start the MQSeries Workflow.

1. Log on as `fmc`.
2. To start the MQSeries Workflow, type: `CMBWFSUNStart.sh`. You will see console messages being reported while the MQSeries Workflow is starting up.
3. You will be prompted to enter the EIP Administrator user id (i..e, `icmadmin`) and password in order to start up the EIP collection points monitor.

The EIP collection points monitor will report its startup status via the console. You could modify the line where the CMBWFSUNStart.sh invokes the cmbupes81.sh to give it the user id and password, so you will not be prompted for user id and password next time you run the CMBWFSUNStart.sh script. Type cmbupes81.sh ñh to see possible options.

Tip: If you do not require the collection point functionality, enter ’quit’ to shutdown the UPES server. Shutting down the UPES server does not shut down the MQSeries Workflow.

Tip: The default MQSeries Workflow system administrator (not configuration administrator) id is ADMIN with default password as ″password″. You would want to change it later for security reason. To do that, first start the MQSeries Workflow and use the fmcautil utility to connect to the Workflow system to change the password. After you have done that, be sure to modify the CMBWFSUNStart.sh to reflect your changes. Here are the steps:

1. `fmcautil ñu admin ñp password`
2. `Select u, p to change your password and then exit the utility`
3. Update the `CMBWFAIXStart.sh`. For example:

```
fmcxspea -y=$ConfigurationID -u=$RunTimeAdminID -p=myPassword -f &
```

Chapter 24. Performing pre-installation steps on Solaris

In addition to installing all the necessary prerequisites, you need to complete the following tasks before installing Content Manager and Enterprise Information Portal:

- “Confirm the correct version of Java”
- “Create user IDs”
- “Update the .profiles for the new user IDs” on page 347
- “Create a userprofile file for Content Manager environment settings” on page 347
- “Configure Secure Sockets Layer (SSL) for IBM HTTP server” on page 348
- “Create a staging directory for the resource manager” on page 353
- “Establish the database environment before starting the installation” on page 354

If you had a previous installation of the Content Manager V8 software, be sure to uninstall the product(s) and clean up your environment. Some product files such as configuration files and the databases are purposely left behind after uninstalling. This may affect the success of your installation.

Confirm the correct version of Java

To confirm that you have the correct version of Java, execute the command:

```
# java -version
```

Make sure that the java version 1.3.0 or later is used.

```
java version "1.3.1_02"
```

Create user IDs

You need to create three different user IDs to use with Content Manager and Enterprise Information Portal, as follows:

- Library server ″administration″ user ID (such as `icmadmin`) if you are installing a library server on this workstation. This user ID **must** be part of the DB2 Admin group.
- ″Database connection″ user ID (such as `icmconct`) if you are installing a library server on this workstation. (This should be a regular user ID with normal privleges, not part of the DB2 Admin group.)

- Resource manager ″administration″ user ID (such as `rmadmin`) if you are installing a resource manager on this workstation. This user ID **must** be part of the DB2 Admin group.

The icmadmin user ID and the rmadmin user ID need to be part of the DB2 Admin group. Follow these steps to create each user as part of the db2 administration server group named db2iadm1 (that is, the same group used for your db2 instance):

__ 1. Create the user IDs:

```
useradd -g staff -G db2iadm1
icmadminuseradd -g staff -G db2iadm1
```

```
rmadminuseradd icmconct
```

__ 2. Assign initial passwords. Set the password value to ″password″ for simplicity. The first login will not prompt you to change the passwords. You can change passwords later, once logged on as the new user, by issuing the following command. (In order to follow this guide with ease, keep the password value as ″password″):

```
passwd icmadmin
```

```
passwd rmadmin
```

```
passwd icmconct
```

__ 3. Perform initial login for added users. You are prompted to change the password for the added users.

```
login icmadmin
```

```
login rmadmin
```

```
login icmconct
```

Very important: You need to remember these user IDs and their passwords for entry during the installation. We remind you about them during the installation (at the time that you need to enter them). You can record their names here:

Table 120. Administration and connection IDs

	Default name / information	**Record your value here**
Library server database administration ID	icmadmin	
Library server database administration ID password		
Database connection ID	icmconct	
Database connection ID password		

Table 120. Administration and connection IDs (continued)

	Default name / information	Record your value here
Resource manager database administration ID	rmadmin	
Resource manager database administration ID password		

Update the .profiles for the new user IDs

Add the following line to /export/home/icmadmin/.profile and /export/home/rmadmin/.profile files:

```
. /export/home/db2inst1/sqllib/db2profile
```

Note the space between the period (.) and the first slash (/). This establishes the DB2 environment associating the users with the db2inst1 DB2 instance.

Update the DB2 instance profile.env file

If the data is not already in the file, add the following lines to the /export/home/db2inst1/sqllib/profile.env file:

```
DB2ENVLIST='LIBPATH ICMROOT ICMDLL ICMCOMP CMCOMMON'
DB2COMM='tcpip'
DB2AUTOSTART='TRUE'
```

Create a userprofile file for Content Manager environment settings

Create a file or update the file: /export/home/db2inst1/sqllib/userprofile containing the following information:

```
ICMROOT=/opt/IBMicm
ICMDLL=/export/home/db2fenc1
ICMCOMP=/opt/SUNWspro/bin
CMCOMMON=/opt/IBMcmb/cmgmt
PATH=$PATH:$ICMROOT/bin/DB2
LD_LIBRARY_PATH=$ICMROOT/lib:$ICMROOT/inso:$LD_LIBRARY_PATH
export ICMROOT ICMDLL ICMCOMP CMCOMMON PATHLD_LIBRARY_PATH
```

Do not modify /export/home/db2inst1/sqllib/db2profile, since this file can be overwritten by the application of a DB2 fixpack. Instead:

1. Put any necessary modifications in userprofile.
2. When db2profile is invoked, it runs userprofile.
3. When db2profile runs userprofile, it causes all settings added to the userprofile to be set for users whose profile exporting the db2profile.

Configure Secure Sockets Layer (SSL) for IBM HTTP server

If you installed WebSphere on this workstation, you need configure Secure Sockets Layer (SSL) for IBM HTTP Server.

This section explains how to configure Secure Sockets Layer (SSL) for IBM HTTP Server on a Solaris server to establish secure connections. The resource manager, which requires a web server such as IBM HTTP Server, requires SSL in order to fully communicate with the system administration client. It is important that you follow these instructions very carefully.

Once configured for SSL, you need to enable both http and https access for the resource manager.

See the IBM HTTP Server documentation for the most recent and complete details.

Overview of Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is an encryption system used on servers to ensure that data transferred between a client and a server remains secure and private.

For a server and client to use SSL for secure communications, the server must have two things:

Key pair
A Key pair consists of public and private keys. The keys are used for encryption and decrypting of messages to ensure privacy and confidentiality in transmissions across the internet.

Certificate
The certificates is used for authentication or verification of identity. A certificate can be either self-signed certificate or an issued certificate:

Self-signed
A certificate that you create for your own private Web network

Issued Provided (issued) to you by a *certificate authority* (CA) or by a *certificate signer*.

SSL uses a security handshake to initiate a secure connection between the client and the server. During the handshake, the client and server agree on the keys they will use for the session and the method for encryption. The client authenticates the server using the server certificate.

After the handshake, SSL is used to encrypt and decrypt all of the information in both the HTTPS (a unique protocol that combines SSL and HTTP) request and the server response, including:

- The URL that the client is requesting
- The contents of any form being submitted
- Access authorization information (like user names and passwords)
- All data sent between the client and the server

Configuring secure connections

To have a secure network connection, you need to complete the following four procedures:

__ 1. Create a new key database (if one does not already exist) and a key.

__ 2. Receive a server certificate from a certificate authority or create a self-signed server certificate using the IBM Key Management Utility (IKEYMAN).

__ 3. Set up SSL using the IBM Administration Server.

__ 4. Test the server installation and configuration.

Creating a new key database

A key database is a file that the server uses to store one or more key pairs and certificates. You can use one key database for all your key pairs and certificates, or create multiple databases. You can create a new key database or you can use an existing key database. If you want to use an existing key database, you can go on to "Creating a self-signed certificate" on page 350.

If you want to create a new key database, continue below.

To create a new key database:

__ 1. Start by creating a directory to store the *keys* database files:

```
mkdir /opt/IBMHTTPD/keys
```

This directory must pre-exist when you actually create the files.

__ 2. Enter `ikeyman` on the command line to start the Key Management utility.

__ 3. Click **Key Database File ⟶ New**.

__ 4. In the New window that opens:

a. Enter your key database name in the **File name** field (for example: **key.kdb**)

b. Enter the path to the keys folder (that you created in step 1) in the **Location** field

c. Click **OK**

__ 5. When the Password Prompt window opens:

__ a. Create a password. (A minimum of six characters is required.)

__ b. Confirm the password.

__ c. **Very important:** Select the **Stash the password to a file** check box.

__ d. Click **OK**.

Password Strength guidelines:
You can see the *strength* of the password change by the number of key symbols that appear (up to five keys).You can see five keys appear after you enter a complicated key with mixed-case alpha-numeric characters that include special characters, such as the following example: `MickeyMouse43@#0243`

__ 6. An information window opens to tell you that the password has been encrypted and saved. Click **OK**.

__ 7. Close the IBM Key Management window (**Key Database File → Exit**).

Creating a self-signed certificate

Use `IKEYMAN` to create a self-signed server certificate to enable SSL sessions between clients and the server. Use this procedure if you are acting as your own CA for a private Web network.

__ 1. Enter `ikeyman` on a command line to start the Key Management utility .

__ 2. Click **Key Database File → Open**.

__ 3. In the Open dialog box, enter your key database name (for example: `/opt/IBMHTTPD/keys/key.kdb`), then click **Open**.

__ 4. When the Password Prompt window opens, enter your password (that you created in the previous section) and click **OK**.

__ 5. Select **Personal Certificates** from the dropdown list in the **Key Database content** frame, then click the **New Self-Signed...** button.

__ 6. In the Create New Self-Signed Certificate window, you need to know the following information for these fields (the other fields are self explanatory):

Key label
Set your Key label to**icmrm**

Common name
Enter the fully qualified host name of the Web server as the common name (for example: www.myserver.com).

Organization
You need to put some information in this field (for example: the name of your company or organization).

__ 7. When you have completed this panel, click **OK**.

__ 8. You can verify that the new Personal Certificate was created successfully and its name appears in the Personal Certificate panel (for example *icmrm).

__ 9. After creating the self-signed certificate, confirm that all necessary files have been created. In the /opt/IBMHTTPD/keys directory, you should find four files:

```
key.kdb
key.sth
key.crl
key.rdb
```

If you are missing the key.sth file, you forgot to stash the password to a file. Go back and repeat “Creating a new key database” on page 349. Make sure that you check the box to stash the password after you create it.

__ 10. You are now ready to set up SSL using the IBM HTTP administration server.

Close the IBM Key Management window (**Key Database File → Exit**).

Setting up SSL using the IBM HTTP Administration Server

To set up SSL for Solaris:

__ 1. Backup the current configuration file /usr/HTTPServer/conf/httpd.conf:

```
cp -p /opt/IBMHTTPD/conf/httpd.conf
/opt/IBMHTTPD/usr/HTTPServer/conf/httpd.conf.save
```

__ 2. Add the following rows into the httpd.conf file as the first item of the Dynamic Shared Object (DSO) Support:

```
ClearModuleList
AddModule mod_so.c
LoadModule ibm_app_server_http_module
   /opt/WebSphere/AppServer/bin/mod_ibm_app_server_http.so
LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so
```

__ 3. Comment the ClearModuleList line under the stanza of AddModule and under this line add the reference to mod_ibm_ssl.c:

```
#ClearModuleList
AddModule mod_ibm_ssl.c
....
....
AddModule  mod_setenv_if.c
```

Note: This step may vary if this file has been modified before. If there are additional ClearModuleList commands in the file, then comment them all out except for the one that appears closest to the top of the file (this includes the one you just created).

__ 4. Add the port number for the virtual server just below the ″Port 80″ statement. The default port number for SSL is 443:

```
Port 80
Port 443
```

__ 5. Add the port number for the virtual server just below the ″Listen 80″ statement. The default port number for SSL is 443:

```
Listen 80
Listen 443
```

__ 6. Check that you have defined the ServerName directive. Change the hostnames in red to the name of your machine, example:

```
ServerName homer.svl.ibm.com
```

__ 7. Add following text-block to the end of the `httpd.conf` (after adjusting hostname in red):

```
WebSpherePluginConfig
    /opt/WebSphere/AppServer/config/plugin-cfg.xml
<VirtualHost "homer.stl.ibm.com:443 (homer)">
ServerName homer.stl.ibm.com
DocumentRoot /opt/IBMHTTPD/htdocs/en_US
Keyfile /opt/IBMHTTPD/keys/key.kdb
SSLV2Timeout 100
SSLV3Timeout1000
SSLEnable
SSLClientAuth none
SSLServerCert icmrm
SSLCipherSpec 39
SSLCipherSpec 3A
SSLCipherSpec 62
SSLCipherSpec 64
</VirtualHost>
```

__ 8. Save the `httpd.conf` file

__ 9. Check for the syntax

```
/opt/IBMHTTPD/bin/apachectl configtest
```

__ 10. Restart the server.

```
/opt/IBMHTTPD/bin/apachectl graceful
```

__ 11. Test the server installation:

- __ a. Test the http connection:

  From a web browser enter the URL: `http://<hostname>`

- __ b. Test the https (SSL) connection:

  From a web browser enter the URL: `https://<hostname>`

If SSL is not working, check `/opt/IBMHTTPD/logs/error_log` for messages. A common error message is:

```
mod_ibm_ssl: GSK could not initialize, Invalid password for keyfile
```

In this case, be sure you chose to stash the password when the key database was created (using the ikeyman utility).

Additional steps for WebSphere Application Server, Version 4 Advanced Edition (AE)

If you have WebSphere Application Server Advanced Edition (AE) installed then the Web Server Plugin needs to be generated with SSL information:

__ 1. Make sure that the WebSphere Application Server (WAS) service is started.

__ 2. Invoke the WebSphere Application Administrative Console.

__ 3. Click **Virtual Hosts** in the tree on the left frame of the console Click the **General** tab on the right frame of the console Click **Add**

__ 4. Enter ***:443** in the text area that appears (that's an asterisk, a **colon**, then the numbers 443).

__ 5. Click **Apply**

__ 6. Click **Nodes** (to expand that part of the tree)

__ 7. Right click `<your hostname>` in the tree on the left frame

__ 8. Click **Regen Webserver Plugin**

__ 9. Restart the IBM HTTP Server and the WebSphere Application Server so that the latest plugin information takes effect.

Testing the server installation and configuration

After configuring the Secure Sockets Layer, you should test the server installation:

__ 1. Start WebSphere as follows:

for AES

```
/opt/WebSphere/AppServer/bin/startServer.sh
```

for AE

```
/opt/WebSphere/AppServer/bin/startupServer.sh
```

__ 2. Test the http connection:

```
/http://<hostname>/icmrm/snoop
```

__ 3. Test the https (SSL) connection:

```
/https://<hostname>/icmrm/snoop
```

Create a staging directory for the resource manager

During the Content Manager installation, you are prompted to provide the staging area directory and its mount point. The installation program assumes you have already created this directory:

```
mkdir /export/home/ubosstg
```

Establish the database environment before starting the installation

It is **very important** that you establish the DB2 environment for CM by following hte instructions to set up the userprofile in the sqllib directory (refer to page 321). Running db2profile sets the PATH and CLASSPATH and also identifies the DB2 instance that CM will use: Be sure the

```
. /export/home/db2inst1/sqllib/db2profile
```

was run as root before you install CM. **DO NOT forget this step; if you do, Content Manager will not install successfully.**

Chapter 25. Installing Content Manager components on Solaris

This section is a guide for installing the following Content Manager components on Sun Solaris:

- Library server
- Resource manager
- The Information center

Information for installing the other client components are covered in the following sections:

- Chapter 15, “Installing the Content Manager Client for Windows”, on page 205
- Chapter 29, “Installing Content Manager eClient on Solaris”, on page 425

Before you begin

Before you begin the Content Manager installation:

1. There are special instructions provided for the following required program products:

   IBM DB2 Universal Database or Oracle

   An IBM DB2 Universal Database or an oracle database is required for the library server and the resource manager.

   If you have not already installed your database application:

   - See “IBM DB2 Universal Database” on page 328 for instructions for installing your DB2 database on the workstation.

     The database must be installed on your workstation **before** you begin the installation of the Content Manager components.
   - See “Oracle database on a Solaris system” on page 335 for instructions for installing your Oracle database on the workstation.

     If the library server application and the library server database will be installed on separate machines:

     a. The library server database **must be created before** the library server application component can be installed.
     b. The library server database on the remote Oracle server must be up and running and have an active Oracle listener

associated with it. DB2 will connect to the Oracle database during the library server application inatallation using the tnsnames Net8 protocol.

IBM DB2 Universal Database client software

For Oracle/resource manager installations, IBM DB2 client software is required to be installed. (The DB2 JDBC drivers are needed for communication of the resource manager with the library server.)

DB2 Text Information Extender (TIE)

Text Information Extender (TIE) or DB2 Net Search Extender (NSE) is required if you plan to use the Text Search feature.

See "IBM DB2 Net Search Extender (NSE) and Text Information Extender (TIE)" on page 338 for instructions for installing Text Information Extender (TIE).

NSE or TIE must be installed on the same workstation as the library server. (NSE must be installed on the same workstation as the library server application or Oracle.)

IBM WebSphere Application Server (WAS)

IBM WebSphere Application Server is required for the resource manager.

See "IBM WebSphere Application Server (WAS)" on page 339 for instructions for installing and configuring WAS on the workstation. 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.

Tivoli Storage Manager

Chapter 30, "Installing and Configuring Tivoli Storage Manager (TSM)", on page 431 provides the instructions for installing and configuring TSM. TSM is an optional feature that provides long-term storage on devices other than the fixed disks attached to the resource manager. It is installed after the resource manager component is installed.

2. Ensure that your system meets all of the memory, hardware, and all other software requirements to install Content Manager. Refer to "Solaris requirements" on page 62 for a summary of these requirements.
3. Make sure that the following products that are shipped with Solaris are installed on your machine:
   - TCP/IP
   - Solaris windows
   - Unicode converter (bos.iconv.ucs.pc), which includes:
     - Common Language to Language Converters

  - Unicode Converters for Solaris Code Sets
  - Unicode Converters for Additional PC Code Sets
  - Unicode Converters for EBCDIC Code Sets
4. Make sure that the locale the install program runs under is the same as the one the administration ID's of the selected components have. Otherwise, during runtime, the correct message files and language dependent files may not be available. For example, when you start the Solaris install program, the LANG environment variable is set to ″En_US″, but the locale for the Library Server Administration ID is set to ″en_US″. In this case, only the message files of ″En_US″ locale are installed. Consequently, when you start the Library Server, you will get error message indicating that the message cannot be resolved. This is a minor problem for the English locale but could be a problem to locales such as Italian, Japanese, and others when the regional character sets is different between ″it_IT″ and ″IT_IT″, for example.

Installing Content Manager on Solaris

To start the installation, complete the following steps:

1. Verify that you have created the three necessary user IDs that are needed for the installation:
   - Library server ″administration″ user ID (such as `icmadmin`) if you are installing a library server on this workstation. This user ID **must** be part of the DB2 Admin group.
   - ″Database connection″ user ID (such as `icmconct`) if you are installing a library server on this workstation. (This should be a regular user ID with normal privleges, not part of the DB2 Admin group.)
   - Resource manager ″administration″ user ID (such as `rmadmin`) if you are installing a resource manager on this workstation. This user ID **must** be part of the DB2 Admin group.

   If you do not have the three user IDs, see “Create user IDs” on page 345for detailed instructions for creating them.
2. Modify .profile of `icmadmin` and of `rmadmin` to include the following lines:

   ```
   ICMROOT=/opt/IBMicm

   ICMDLL=$db2fence home (for example /export/home/db2fence1)

   ICMCOMP=/opt/SUNWspro/bin

   CMCOMMON=/opt/IBMcmb/cmgmt

   PATH=$PATH:$ICMROOT/bin/DB2

   LD_LIBRARY_PATH=$ICMROOT/lib:$ICMROOT/inso:/opt/SUNWspro/lib:
   /usr/lib:$LD_LIBRARY_PATH

   export ICMROOT ICMDLL ICMCOMP CMCOMMON PATH LD_LIBRARY_PATH
   ```

   Where:

ICMROOT is the Content Manager product install location

ICMDLL is the DB2 fence location (This is set to home of DB2fence because the fenceID creates the DLL dynamically at run time)

ICMCOMP is the Forte C++ compiler location

CMCOMMON is the shared area for Content Manager and Enterprise Information Portal configuration files

3. Add these lines to .profile of `icmadmin` and of `rmadmin` (if they are not already there)

   ```
   if [[ -e $DB2INSTANCE HOME/sqllib/db2profile ]] then
   . $DB2INSTANCE HOME/sqllib/db2profile
   fi
   ```

   Where: `DB2INSTANCE HOME` is the home directory of the DB2 instance

4. Modify `$DB2INSTANCE HOME/sqllib/profile.env to have the following lines` (if `profile.env` does not exist, create it):

   ```
   DB2ENVLIST='LD_LIBRARY_PATH ICMROOT ICMDLL ICMCOMP CMCOMMON'
   DB2COMM='tcpip'
   ```

5. Shut down any DB2 applications, then stop and start DB2 with one of the following procedures:
   - If you are installing a library server on this machine, login as a the library server admininistrator (for example: icmadmin) to shut down any open DB2 applications, then stop and start DB2 with the same user ID.
   - If you are only installing a resource manager on this machine, login as a the resource manager admininistrator (for example: rmadmin) to shut down any open DB2 applications, then stop and start DB2 with the same user ID.
   - If you are installing both a library server and a resource manager, and if they are being installed against separate DB2 instances, you need to shut down DB2 applications, then stop and start DB2 using both administrator IDs (for example: icmadmin and rmadmin).

Important

a. Whenever you start Content Manager, start it with the library server user ID (<icmadmin>) or the resource manager user ID (<rmadmin>) to ensure that the Content Manager applications can reference required environment variables, which are exported through the profiles of those administrators.

b. Whenever you start WebSphere Application Server for the resource manager, make sure that you have the following environment variable set as follows:

```
EXTSHM=ON
```

6. **For Oracle only:** Make the library server user ID that was created during the installation of DB2 a member of the same group as the Oracle user ID. (For example: make the user ID ICMADMIN a part of the *oinstall* group).
7. **For Oracle only:** Grant **Write permission** for the group in the previous step (for example: *oinstall*) to the `tnsnames.ora` file, located in the directory specified by the Oracle environment variable `TNS_ADMIN`. During the Content Manager installation process, you will be prompted for the value of `TNS_ADMIN`. This value must be consistent with the Oracle installation that you intend for use with Content Manager.
8. **For Oracle only:** Verify that the library server database is up and running by logging on to your Oracle client machine:

   ```
   tnsping LS db name.Oracle server domain name
   ```

   If the connection is successful, proceed with the library server application installation. If the connection is not successful, correct the TNS errors reported by Oracle before continuing:

   a. Check the `tnsnames.ora`, `listener.ora`, and `sqlnet.ora` files on your Oracle machine for proper configuration.

   b. Recycle the Oracle listener on your Oracle server (if necessary) by performing the following steps:

   ```
   lsnrctl stop
   lsnrctl start
   ```

   c. Issue the following command to your Oracle server to ensure that your library server database is associated with the active listener:

   ```
   lsnrctl status
   ```
9. **For Oracle only:** If you experience connectivity problems , for each HOST in the DESCRIPTION section of the `tnsnames.ora` file, you might need to update the `hosts` file:

   ```
   /etc/hosts
   ```

Whether you update this file or not depends on how TCP/IP is configured on your network. Part of the network must translate the remote host name specified in the DESCRIPTION section in the `tnsnames.ora` file to an address. If your network has a named server that recognizes the host name, you do not need to update the TCP/IP `hosts` file. Otherwise, you need an entry for the remote host. See your network administrator to determine how your network is configured.

10. Stop the IBM HTTP Server service.
11. Log in as root (or as a user with root authority)
12. Make sure that your Java JRE Version 1.3 is in the PATH, for example:

    ```
    $JAVA_HOME/bin:$JAVA_HOME/jre/bin:$PATH
    ```
13. Insert the CD-ROM into your CD-ROM drive.
14. Mount your Content Manager CD-ROM, for example:

    ```
    mount -F hsfs -o ro <device>/mountpoint
    ```

    (an example for <device>, the device drive, could be: `/dev/cd0`)
15. Change to the directory where the CD-ROM is mounted by entering the `cd /cdrom` command, where `cdrom` is the mount point of your Content Manager installation CD-ROM.
16. As `root`, execute the following command to get db2 into `PATH,CLASSPATH`:

    ```
    . $DB2INSTANCE HOME/sqllib/db2profile
    ```
17. Start the installation wizard by entering the following:

    ```
    ./setup.exe
    ```

Welcome panel

The first panel (Welcome) of the InstallShield Wizard opens.

Click **Next**.

Software License Agreement panel

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

Click **Next** to continue the installation.

Step 1. Select the type of installation

At this window, you decide whether to install all of the available components on this workstation, or to customize the installation by selecting which components to install. **Important:** If you are using Oracle as your database application for Content Manager, you must choose the **Custom** option. If you are using DB2 UDB as your database application, you can choose either the **Full** or the **Custom** option:

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

- Library server
- Resource manager
- Information center

When you click **Next**, after selecting this option, go to "Step LS1. Configure Library Server" on page 362.

Custom

Select **Custom** if you want to select which component(s) to install on this workstation. Click **Next** to continue the installation with "Step 2. Selecting the components to install".

Step 2. Selecting the components to install

The Component Selection window opens, showing you what components are available to install.

Select the components that you want to install. (By default, all components are checked.)

- Click in the box to remove the check mark of the components that you do not want to install.
- Leave a check mark in the box for each component that you want to install.

Click **Next** when you are satisfied with your selections.

Depending on the selections that you made on this panel, go to the page indicated in Table 121.

Table 121. Location of next step

Choices	Go to
Library server with IBM DB2 (either alone or with any, or all, of the other components)	"Step LS1. Configure Library Server" on page 362
Library server with Oracle (either alone or with any, or all, of the other components)	"Step ORA1. Select Library Server Components" on page 369
Resource manager with IBM DB2 only (no other components selected)	"Step RM1. Configure Resource Manager Server" on page 364
Resource manager with Oracle only (no other components selected)	"Step ORA2. Select Resource Manager Components" on page 370
Resource manager with IBM DB2 and Information center	"Step RM1. Configure Resource Manager Server" on page 364

Table 121. Location of next step (continued)

Choices	Go to
Resource manager with Oracle and Information center	"Step ORA2. Select Resource Manager Components" on page 370
Information center only	"Step VE1. Verify the install location" on page 387

Step LS1. Configure Library Server

Skip this step if you are not installing the library server component at this time, and continue with "Step RM1. Configure Resource Manager Server" on page 364.

Enter the following information for your library server database:

Table 122. Library server configuration

Install information	Description	Default name / option	Record your value here
Library server database name	The name of the library server database	ICMNLSDB	
Library server schema name	The library server 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	

Note:

1. This is the Administration ID that you created at the beginning of the install process. See "Create user IDs" on page 345.
2. This is the Database connection ID that you created at the beginning of the install process. See "Create user IDs" on page 345.

When you complete your library server configuration, click **Next**.

Program note:

1. At this time the installation program checks to see if a Content Manager (CM) library server database or an Enterprise Information Portal (EIP) system administration database exist on this workstation.

   If a database exists, the program checks to see if it has the same database name, the same user ID, the same schema name, or the same password that you entered.

   - If (only) a CM library server database already exists, the program asks if you want to overwrite the existing database, keep it, or go back to type in new information for the new database.
   - If (only) an EIP system administration database exists, the program asks if you want to share the database between CM and EIP, or if you want to type in another name for the new CM library server database. The installation program cannot create a new separate library server database with the same name as the system administration database. You must give it a different name than the system administration database.
   - If a shared database between CM and EIP already exists, the program asks if you want to proceed with no change to the existing database, or to go back and enter a new information for the database that you want to create.
2. Also, during the time that the library server is being installed, a program called ″library server monitor″ is being created automatically. The library server monitor program's job is to detect the availability of resource managers to a library server database (among other things that are listed in the section called "Running the library server monitor program" on page 498.).

   If the library server monitor program ever stops running abnormally, then you need to restart it by using the procedure that is also described in the section called "Running the library server monitor program" on page 498.

Step LS2. Configure Library Server Options

Select the library server options:

Table 123. Library server configuration options

Install information	Description	Default name / option	Record your value here
Name of library server ID	Enter the name of the library server ID (Range = 1 to 99)	1	
Enable Unicode (check box)	Check this box to enable Unicode .	(not checked/No)	

Table 123. Library server configuration options (continued)

Install information	Description	Default name / option	Record your value here
Enable text search (check box)	Check this box if you want to use the Text Search feature. [1]	(not checked/No)	

Note:

1. You must have the DB2 Text Information Extender (TIE) or DB2 Net Search Extender (NSE) installed to use Text Search.

Click **Next** to continue to the next window.

Step RM1. Configure Resource Manager Server

Skip this step if you are not installing the resource manager component at this time, and continue with "Step CNLS1. Connect Library Server To Resource Manager" on page 366

Enter the identification and authentication information for the resource manager:

Table 124. Configuring the resource manager server

Install information	Description	Default name / option	Record your value here
Resource manager database name	The name of the resource manager database	RMDB	
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>	

Note:

1. This is the Administration ID that you created at the beginning of the install process. See "Create user IDs" on page 345.

When you complete your resource manager configuration, click **Next**.

Program 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.

Step RM2. Configure Resource Manager Server Options

Enter the information for the resource manager mount point, and staging area path:

Table 125. Resource manager server options

Install information	Description	Default name / option	Record your value here
Mount point	Location of the storage area that is used for storing objects	/export/home[1]	
Staging area path	Location of the storage area that is used for staging LAN Cache objects or TSM objects	/export/home /ubosstg/	

Note:

1. This is where resource manager objects are stored. Ensure that you have sufficient space on this file system.

Click **Next** to continue to the next window.

Step RM3. Deploy Resource Manager With WebSphere Application Server

Enter the following information to identify the application server that your resource manager will use:

Table 126. Deploying the resource manager

Install information	Description	Default name / option	Record your value here
WAS home	Location of the WebSphere Application Services program[1]	/opt/WebSphere /AppServer	
Web application path	The web path to the WebSphere application server	/icmrm	

Table 126. Deploying the resource manager (continued)

Install information	Description	Default name / option	Record your value here
Web application name	The name of the Web application	icmrm	
Services port	Enter a port number (the first of five numbers) to be used for resource manager components (migrator, purger, stager, replicator, and asynchronous recovery)	<recommendPort> The recommended port number is displayed on the panel[2].	
Node name	Enter the node name for this resource manager application	<current machine node name>	
WAS administrator user name	Enter the WAS administrator user ID	was_admin	
Password (two fields)	Enter and confirm the password for the WAS Admin user name	<password>	
Application server name [3]	The name of the WAS AE application server[3]	ICMRM	

Note:

1. The installation program deploys icmrm.war only if WebSphere Version 4.0.3 (or later) is installed on this workstation. (See the README for the latest information.)
2. You can enter a port number other than the recommended default number. However, it must be the first number of five available contiguous port numbers.
3. **Special use field:** This field is only used if WebSphere Application Server Advanced Edition (AE) is installed on this workstation.

Click **Next** to continue to the next window.

Step CNLS1. Connect Library Server To Resource Manager

Skip this step if any one of the conditions listed in Table 127 on page 367 are true, and continue with the step indicated. Otherwise, continue below.

Table 127. Location of next step

Condition	Continue with (go to)
If you are not installing a library server or a resource manager at this time	"Step VE1. Verify the install location" on page 387
If you are installing a resource manager, **but not** a library server at this time	"Step CNRM. Connect Resource Manager To Library Server" on page 368

Enter the information about the resource manager that the library server needs to connect to it:

Table 128. Connect library server to resource manager

Install information	Description	Default name / option	Record your value here
Resource manager server host name	The fully qualified host name of the workstation that contains the resource manager	<hostName>	
Resource manager database name	The name of the resource manager database	RMDB	
Web application port number	The port number for the Web Application Server	80	
Secure Web application port (HTTPS)	Port number for the resource manager to communicate with the system administration client	443	
Web application path	Same as the path entered in "Step RM3. Deploy Resource Manager With WebSphere Application Server" on page 365	/icmrm	
Resource manager server operating system (drop-down list of available choices)	The operating system of the workstation where the resource manager is located	<platform>	

Table 128. Connect library server to resource manager (continued)

Install information	Description	Default name / option	Record your value here
Token duration (hours)	The amount of time (in hours) that a connection between the library server and the resource manager can stay active until it is discarded by the system. (Can be modified later with the system administration client tools.)	48	

Click **Next** to continue to the next window.

Step CNLS2. Connect Library Server To Resource Manager Part 2

Skip this step if the library server and the resource manager are being installed on the same machine.

Enter the resource manager database connection ID and password:

Table 129. Resource manager connection ID

Install information	Description	Default name / option	Record your value here
Resource manager database administration ID	See Note 1 (below).	rmadmin	
Password	See Note 1 (below).	<password>	
Note: 1. These are the same values that were entered during "Step RM1. Configure Resource Manager Server" on page 364.			

Click **Next** to continue to the next window.

Step CNRM. Connect Resource Manager To Library Server

Skip this step if you are not installing a resource manager at this time, or if the library server and the resource manager are being installed on the same machine.

Enter the information about the library server that the resource manager needs to connect to it:

Table 130. Connect resource manager to library server

Install information	Description	Default name / option	Record your value here
Library server host name	The host name of the workstation that contains the library server	<host name>	
Library server database name	See Note 1 (below).	ICMNLSDB	
Library server schema name	See Note 1 (below).	ICMADMIN	
Library server database administration ID	See Note 1 (below).	icmadmin	
Password	See Note 1 (below).	<password>	
Note: 1. These are the same values that were entered during "Step LS1. Configure Library Server" on page 362.			

Click **Next** and continue with"Step LDAP1. Configure Components for LDAP" on page 384.

Step ORA1. Select Library Server Components

Skip this step if you are not installing a library server (with Oracle) on this machine.

Select the library server components to install on this machine, and enter the location of the configuration file:

Table 131. Select library server components

Install information	Description	Default name / option	Record your value here
Library server database	Check this box to install the library server database on this machine	(checked)	

Table 131. Select library server components (continued)

Install information	Description	Default name / option	Record your value here
Library server application	Check this box to install the library server application on this machine	(checked)	
Location of the default configuration settings file	Path to the default configuration settings file[1]	Default	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387			

Click **Next** to continue to the next window.

Step ORA2. Select Resource Manager Components

Skip this step if you are not installing a resource manager (with Oracle) on this machine.

Select the resource manager components to install on this machine, and enter the location of the configuration file:

Table 132. Select resource manager components

Install information	Description	Default name / option	Record your value here
Library server database	Check this box to install the resource manager database on this machine	(checked)	
Library server application	Check this box to install the resource manager application on this machine	(checked)	
Location of the default configuration settings file	Path to the default configuration settings file[1]	Default	

Table 132. Select resource manager components (continued)

Install information	Description	Default name / option	Record your value here
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387			

Click **Next** to continue to the next window.

Step ORA3. Configure Oracle Database (1)

Enter the information for the Oracle database server:

Table 133. Oracle server database

Install information	Description	Default name / option	Record your value here
Base directory for Oracle	This is the fully-qualified path under which all Oracle products can be found.[1]	opt/oracle	
Oracle database server directory	This is the fully-qualified path to your Oracle Enterprise Edition product directory. [1]	opt/oracle/Ora92	
Oracle TNS Names file location	This is the fully-qualified path to the `tnsnames.ora` file in use for the ORACLE_HOME environment variable.[1]	opt/oracle/ora92/network/admin	
Oracle NLS message files location	This is equivalent to your ORA_NLS33 environment variable.[1]	opt/oracle/ora92/ocommon/nls/admin/data	
Oracle JDBC path	Click **Browse** to find the path to the JDBC directory		

Table 133. Oracle server database (continued)

Install information	Description	Default name / option	Record your value here
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387			

Click **Next** to continue to the next window.

Step ORA4. Configure Oracle Database (2)

Enter information for the Oracle database server:

Table 134. Oracle database

Install information	Description	Default name / option	Record your value here
Oracle database server version	Select the version of the installed Oracle software[1]	9.2.0.1 OR higher	
Password (two fields)	Enter and confirm the password for the Oracle SYSTEM and SYS user IDs[1]	<password>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387			

Click **Next** to continue and go to the first step indicated by the following questions:

1. Are you installing a library server database or a library server application on this machine?

   If **yes**, go to question 2.

   If **no**, go to question 3.

2. Are you installing a library server application on this machine?

   If **yes**, go to "Step OLS1. Configure Library Server Application (1)" on page 373.

   If **no**, go to "Step OLS6. Configure Library Server Database (1)" on page 376.

3. Are you installing a resource manager database on this machine?

If **yes**, go to “Step ORM1. Configure Resource Manager Database (1)” on page 379.

If **no**, go to “Step ORM5. Configure Resource Manager Application (1)” on page 382.

Step OLS1. Configure Library Server Application (1)

Skip this step if you are not installing a library server application on this machine, and go to “Step OLS6. Configure Library Server Database (1)” on page 376.

Enter the information for the library server application to connect to the library server database:

Table 135. Configure library server connections

Install information	**Description**	**Default name / option**	**Record your value here**
Library server database name	Enter the library server database name	ICMNLSDB	
Library server schema name	Enter the library server schema name	ICMADMIN	
Library server database administration ID	This is the user ID that is used to administer your Content Manager library server[1]	oraadmin	
Password (two fields)	Enter and confirm the password	<password>	

Notes:

1. For more information about this field, see “Oracle - expanded information for installation panel fields” on page 387

Click **Next** to continue to the next window.

Step OLS2. Configure Library Server Application (2)

Enter the information for library server database connection ID:

Table 136. Library server connection ID

Install information	Description	Default name / option	Record your value here
Library server database connection ID	Enter the library server database connection ID	ICMCONCT	
DB2 instance owner ID	This is the ID that you created prior to installing the DB2 product.[1]	DB2INST1	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387

Click **Next** to continue to the next window.

Step OLS3. Configure Library Server Application (3)

Enter the information for library server application options:

Table 137. Library server application options

Install information	Description	Default name / option	Record your value here
DB2 database location	Fully qualified path to the location of the DB2 database that is used with this Oracle database		
Enable unicode	Select to enable unicode	(not checked)	

Click **Next** to continue to the next window.

Step OLS4. Configure Library Server Application (4)

Enter the information for connecting the library server application to the resource manager server:

Table 138. Library server application connection to resource manager

Install information	Description	Default name / option	Record your value here
Resource manager server host name	Enter the resource manager server host name	<hostname>	
Resource manager database administration ID	Enter the resource manager database administration ID	RMADMIN	
Password (two fields)	Enter and confirm the password for the resource manager database administration ID	<password>	

Click **Next** to continue to the next window.

Step OLS5. Configure Library Server Application (5)

Enter more information in this window for connecting the library server application to the resource manager server:

Table 139. Library server application connection to resource manager

Install information	Description	Default name / option	Record your value here
Web application name	Enter the web application name	icmrm	
Web application path	Enter the path for the web application	/icmrm	
Web application port	Enter the port number for the web application	80	
Secure web application port (HTTPS)	Enter the port number for the secure web application	443	

Table 139. Library server application connection to resource manager (continued)

Install information	**Description**	**Default name / option**	**Record your value here**
Token duration (hours)	The amount of time (in hours) that a connection between the library server application and the resource manager can stay active until it is discarded by the system. (Can be modified later with the system administration client tools.)	20	

Click **Next** to continue and go to the first step indicated by the following questions:

1. Are you installing a library server database on this machine?

   If **yes**, go to “Step OLS6. Configure Library Server Database (1)”.

   If **no**, go to question 2.

2. Are you installing a resource manager database or a resource manager application on this machine?

   If **yes**, go to question 3.

   If **no**, go to “Step LDAP1. Configure Components for LDAP” on page 384.

3. Are you installing a resource manager database on this machine?

   If **yes**, go to “Step ORM1. Configure Resource Manager Database (1)” on page 379.

   If **no**, go to “Step ORM5. Configure Resource Manager Application (1)” on page 382.

Step OLS6. Configure Library Server Database (1)

Skip this step if you are not installing a library server database on this machine, and go to “Step ORM1. Configure Resource Manager Database (1)” on page 379.

Enter information for the library server database:

Table 140. Library server database

Install information	Description	Default name / option	Record your value here
Library server database name	Enter the library server database name	ICMNLSDB	
Library server database location	Enter the fully-qualified path name of the location where you want Oracle to store its internal database files.[1]		
Library server host name	This is the host-only name of the Oracle server where your library server database is created.[1]	<hostname>	
Library server domain name	This is the domain name that is associated with the host name for the library server (in the row above this one).	<xmpl.name.com>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387			

Click **Next** to continue to the next window.

Step OLS7. Configure Library Server Database (2)

Enter more information for the library server:

Table 141. Library server database (more information)

Install information	Description	Default name / option	Record your value here
Oracle listener name	Enter the name of the Oracle listener[1]	LISTENER	
Oracle protocol	Select the protocol from the drop-down list[1]	TCP/IP	

Table 141. Library server database (more information) (continued)

Install information	Description	Default name / option	Record your value here
Oracle listener port	Enter the port number for the Oracle listener[1]	1521	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387

Click **Next** to continue to the next window.

Step OLS8. Configure Library Server Database (3)

Enter the authentication information for the library server database:

Table 142. Oracle database administration ID

Install information	Description	Default name / option	Record your value here
Oracle database administration ID	Enter the Oracle database administration ID[1]	oraadmin	
Password (two fields)	Enter and confirm the password for the Oracle database administration ID[1]	<password>	

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387

Click **Next** to continue to the next window.

Step OLS9. Configure Library Server Database (4)

Select the configuration options for the library server database:

Table 143. Library server database configuration options

Install information	Description	Default name / option	Record your value here
Enable for unicode	Check this box to enable for unicode	(not checked)	

Table 143. Library server database configuration options (continued)

Install information	Description	Default name / option	Record your value here
Mirror database files	Check this box to mirror database files	(checked)	
Mirror directory	Enter (or browse to) the path for the Mirror directory[1]		

Notes:

1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387

Click **Next** to continue and go to the first step indicated by the following questions:

1. Are you installing a resource manager database or a resource manager application on this machine?

   If **yes**, go to question 2.

   If **no**, go to "Step LDAP1. Configure Components for LDAP" on page 384.
2. Are you installing a resource manager database on this machine?

   If **yes**, go to "Step ORM1. Configure Resource Manager Database (1)".

   If **no**, go to "Step ORM5. Configure Resource Manager Application (1)" on page 382.

Step ORM1. Configure Resource Manager Database (1)

Skip this step if you are not installing a resource manager database on this machine, and go to "Step ORM5. Configure Resource Manager Application (1)" on page 382.

Enter information for the resource manager database:

Table 144. Resource manager database

Install information	Description	Default name / option	Record your value here
Resource manager database name	Enter the resource manager database name	RMDB	

Table 144. Resource manager database (continued)

Install information	Description	Default name / option	Record your value here
Resource manager database location	Enter the fully-qualified path name of the location where you want Oracle to store its internal database files.[1]		
Resource manager host name	This is the host-only name of the Oracle server where your resource manager database is created.[1]	<hostname>	
Resource manager server domain name	This is the domain name that is associated with the host name for the resource manager (in the row above this one).	<xmpl.name.com>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387			

Click **Next** to continue to the next window.

Step ORM2. Configure Resource Manager Database (2)

Enter more information for the resource manager:

Table 145. Resource manager database (more information)

Install information	Description	Default name / option	Record your value here
Oracle listener name	Enter the name of the Oracle listener[1]	LISTENER	
Oracle protocol	Select the protocol from the drop-down list[1]	TCP/IP	
Oracle listener port	Enter the port number for the Oracle listener[1]	1521	

Table 145. Resource manager database (more information) (continued)

Install information	Description	Default name / option	Record your value here
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387			

Click **Next** to continue to the next window.

Step ORM3. Configure Resource Manager Database (3)

Enter the authentication information for the resource manager database:

Table 146. Oracle database administration ID

Install information	Description	Default name / option	Record your value here
Oracle database administration ID	Enter the Oracle database administration ID[1]	RMADMIN	
Password (two fields)	Enter and confirm the password for the Oracle database administration ID[1]	<password>	
Notes: 1. For more information about this field, see "Oracle - expanded information for installation panel fields" on page 387			

Click **Next** to continue to the next window.

Step ORM4. Configure Resource Manager Database (4)

Select the configuration options for the resource manager database:

Table 147. Resource manager database configuration options

Install information	Description	Default name / option	Record your value here
Mirror database files	Check this box to mirror database files	(checked)	
Mirror directory	Enter (or browse to) the path for the Mirror directory[1]		

Table 147. Resource manager database configuration options (continued)

Install information	Description	Default name / option	Record your value here
Notes: 1. For more information about this field, see “Oracle - expanded information for installation panel fields” on page 387			

Click **Next** to continue to the next window.

Step ORM5. Configure Resource Manager Application (1)

Skip this step if you are not installing a resource manager application on this machine, and go to “Step LDAP1. Configure Components for LDAP” on page 384.

Enter information for the resource manager application:

Table 148. Resource manager application

Install information	Description	Default name / option	Record your value here
Web application server name	Enter the web application server name	icmrm	
Web application name	Enter the web application name	icmrm	
Web application path	Enter (or browse to) the path for the web application	/icmrm	
Node name	Enter the node name for this resource manager application	<current machine node name>	
WAS administrator user name	Enter the WAS administrator user ID	was_admin	
Password (two fields)	Enter and confirm the password for the WAS Admin user name	<password>	

Click **Next** to continue to the next window.

Step ORM6. Configure Resource Manager Application (2)

Enter information for the resource manager appliction:

Table 149. Resource manager application mount point and staging area

Install information	Description	Default name / option	Record your value here
Mount point	Enter the location of the storage area that is used for storing objects		
Staging area path	Enter the location of the storage area that is used for staging LAN Cache objects or TSM objects		
Resource manager services port	Enter a port number (the first of five numbers) to be used for resource manager components (migrator, purger, stager, replicator, and asynchronous recovery)	<recommendPort> The recommended port number is displayed on the panel[1].	
Note: 1. You can enter a port number other than the recommended default number. However, it must be the first number of five available contiguous prot numbers.			

Click **Next** to continue to the next window.

Step ORM7. Configure Resource Manager Application (3)

Enter information for the resource manager to connect to the library server:

Table 150. Connect the resource manager to the library server

Install information	Description	Default name / option	Record your value here
Library server host name	Enter the library server host name	<hostname>	
Library server database name	Enter the library server database name	ICMNLSDB	

Table 150. Connect the resource manager to the library server (continued)

Install information	Description	Default name / option	Record your value here
Library server schema name	Enter the library server schema name	ICMADMIN	

Click **Next** to continue to the next window.

Step ORM8. Configure Resource Manager Application (4)

Enter additional information for the resource manager to connect to the library server:

Table 151. Library server application administration ID

Install information	Description	Default name / option	Record your value here
Library server application administration ID	Enter the library server application administration ID	oraadmin	
Password (two fields)	Enter and confirm the password for the library server application administration ID	<password>	

Click **Next** to continue to the next window.

Step LDAP1. Configure Components for LDAP

On this panel, you decide if you want to enable LDAP (Lightweight Directory Access Protocol).

Select the components that you want to enable for LDAP:

Table 152. Enable LDAP options

Install information	Description	Default name / option	Record your value here
Library server (check box)	Check this box to allow user authentication for the library server by an LDAP server	(not checked)	

Table 152. Enable LDAP options (continued)

Install information	Description	Default name / option	Record your value here
Resource manager server (check box)	Check this box to allow user authentication for the resource manager by an LDAP server	(not checked/No)	

Note:

1. If you enabled (or plan to enable) LDAP for your the system administration client (during its installation), it is a good idea to also check the library server check box (to allow user authentication for the library server)

Click **Next** to continue.

Step LDAP2. Define LDAP Server

Skip this step if you did not select to Enable LDAP for any components in the previous step, and continue with "Step VE1. Verify the install location" on page 387.

Enter the information for the LDAP server that you want to use:

Table 153. Define the LDAP server

Install information	Description	Default name / option	Record your value here
LDAP server type (drop-down list of available choices)	Select either **Standard LDAP** or **Active Directory**	Standard LDAP	
Host name	Enter the host name of the LDAP server machine	ldap://ldapServer.ibm.com	
Port	Enter the port number on the LDAP server machine	389	
LDAP server administration ID	Enter the LDAP server administration ID for LDAP on the LDAP server machine	cn = root (default for IBM Directory) <adminId> (default for Active Directory)	

Table 153. Define the LDAP server (continued)

Install information	Description	Default name / option	Record your value here
Password	Enter the password for the LDAP server administration ID	<password>	
Note: 1. Select Standard LDAP for IBM Directory or for Domino NAB.			

Click **Next** to continue to the next window.

Step LDAP3. Configure LDAP Server

Enter configuration information for the LDAP server

Table 154. Configure the LDAP server

Install information	Description	Default name / option	Record your value here
Base distinguished name	Refer to the LDAP documentation for information about the base distinguished name	o=IBM, c=US	
User authentification attribute	Refer to the LDAP documentation for information about the user authentification attribute	cn	
Search scope	During search operations against an LDAP, search at one level or in a subtree fashion[1]	Subtree	
Referral	Choose to **Ignore** or **Follow** a reference to another LDAP server[1]	Ignore	
Note: 1. See the LDAP documentation for more information			

Click **Next** to continue to the next window.

Step VE1. Verify the install location

Verify that the installation information is correct. If any information is incorrect, you can return to previous windows by using the **Back** buttons. Click **Next** to complete the installation.

The Content Manager install program goes to work

The Start Copying Files window opens.

You will see a message that installation has been successful. Click **Finish**.

You can view the installation logs at the following location:

```
/opt/IBMicm/logs
```

Verify the installation

After the installation is complete, you can go to the Windows workstation that has the system administration client installed to verify that the installation is successfull. See “First steps - verify the installation” on page 147.

Oracle - expanded information for installation panel fields

This section is provided to give more detail for the information that is added to specific fields during the installation.

Location of the default configuration settings file

You can re-use an existing `icmlsdb.properties` for the library server (or `icmrmdb.properties` file for the resource manager) file as input to the installation process. If no path is provided, values from a default version of the file will be used by install. You can modify or accept these values during the course of the installation. It is also possible to have a custom-made `icmlsdb.properties` file for the library server (or `icmrmdb.properties` file for the resource manager) for use in deploying a new library server (or Resource Manager). However, this is not recommended due to the importance of the accuracy of the information in the `icmlsdb.properties` for the library server (or `icmrmdb.properties` file for the resource manager) file.

Base directory for Oracle

This is the fully-qualified path under which all Oracle products can be found. During your initial installation of the Oracle product, you were asked for this value during Oracle product installation. This is the ORACLE_BASE environment variable. For example, if you have installed both Oracle Enterprise Edition and the Oracle Universal Installer, you might have a directory tree similar to the following:

```
/opt/oracle/  ---> /opt/oracle/product/8.1.7
                |
                 --> /opt/oracle/oui
```

In this example, /opt/oracle would be the value of your ORACLE_BASE environment variable.

Oracle database server directory

This is the fully-qualified path to your Oracle Enterprise Edition product directory. Under this directory is the Oracle database bin, network, dbs, and other related directories. This is equivalent to your ORACLE_HOME environment variable. In the example above, the ORACLE_HOME value would be /opt/oracle/product/8.1.7

Oracle TNS Names file location

This is the fully-qualified path to the tnsnames.ora file in use for the ORACLE_HOME environment variable that you specified in the previous step. The value for this field is equivalent to your Oracle TNS_ADMIN environment variable. The oracle user ID should have full access to this TNS_ADMIN location. Additionally, this file must have write permissions for the Oracle group so that the db2 instance user ID (which must also be a member of the Oracle group) can update the information for Content Manager.

Oracle NLS message files location

For most customers, this value should be ORACLE_HOME/ocommon/nls/admin/data. It is equivalent to your Oracle ORA_NLS33 environment variable. This setting is intended primarily for customers who have different installations of Oracle on the same machine and utilize different language versions.

Oracle database server version

If you are using any version of Oracle 9.2.0.1 or higher, you should select ″9.2.0.1 or higher″. If you are selecting any version of Oracle 8.1.7.4 or higher, but are not using Oracle 9i, you should select ″8.1.7.4 or higher″. Note that Content Manager does not support Oracle versions of 9i less than 9.2.0.1, nor any versions of 8i less than 8.1.7.4.

Refer to Oracle’s Metalink website for any patchsets and related installation instructions you may need to upgrade your Oracle system prior to installing Content Manager.

Password (for Oracle SYS and SYSTEM)

This is the password that will be *set* for the Oracle-created accounts SYS and SYSTEM. At database creation time, these two internal accounts are set with the password value you provide here. As indicated in Oracle security guidelines, you should differentiate the password used for these accounts after database creation. Setting the passwords provides additional security for the administration of your Oracle database.

Library server database administration ID/Schema name

This will be the user ID used to administer your Content Manager library server. In most cases, this will also be your Library server schema name. Therefore, unless you specifically want to have your library server schema ID separate from your library server administrator ID, these two values will be the same (for example: `icmadmin`).

DB2 instance owner ID

This is the user ID you created prior to installation of the DB2 product. It is the user ID that you specified during installation of DB2 as the DB2 instance user ID. It is also the user ID that you included in the Oracle user ID group. As the user ID that owns a DB2 instance, this user ID, by default, also has `DB2 SYSADM` privileges which are needed to create a DB2 federated database that connects to your Oracle data source.

Library server database location

This should be the fully-qualified path name of the location where you want Oracle to store its internal database files. Additionally, this directory will be used by the installation program to generate intermediate files and database creation log files. It keeps a copy of your `icmlsdb.properties` file for future use. If you will be installing the library server application on an Oracle client machine, you should use `ftp` to connect to this file to your Oracle client machine (to save time and provide default values for the library server application installation). If the directory provided in this field does not exist, the installation program creates it for you. If you are using a directory that already exists, you must ensure that it is owned by the Oracle user ID and has write permissions for the Oracle user ID and Oracle group.

Library server host name

This is the host-only name of the Oracle server on which your library server database will be created. If you are installing a library server database, this will be the host name for the local Oracle server machine. If you are installing the library server application, this will be the host name for the Oracle server machine that *already* contains your library server database.

Oracle listener name

For most Oracle installations, and the value provided by default during an Oracle installation, you will never need to specify a value other than `LISTENER`. If, however, you are certain that your organization uses named listeners and you want to use a specific listener, please enter that name in this field. You can check to see the name of the current, active listener on your Oracle server by issuing the following command:

```
lsnrctl status
```

If the active listener is not the listener you wish to use, you can check your `listener.ora` file on the Oracle server to determine which available, named listener you wish to use. If you want to create a new listener, the listener must be added to your `listener.ora` file before beginning Content Manager installation.

For proper operation of Content Manager, the listener name you specify in this field must be the active listener on your Oracle server at all times.

Oracle protocol
In most cases, you should accept the default value of `TCP/IP` for the Oracle communications protocol to be used. If you choose to select another Oracle-supported protocol, you must verify that your Oracle client/server environment is correctly configured for this protocol using the Oracle `TNSNAMES` naming method and the Oracle Net8 database communications protocol.

Oracle listener port
Most Oracle installations use a default listener port of 1521. If you know that the named listener you wish to use has a different protocol, please specify that value here. You can verify this by referring to your Oracle `listener.ora` file.

Oracle database administration ID
To maximize the security of your library server database and Oracle system, it is good practice to choose a different value for this field than the user ID and password that you provide for the library server administrator user ID and password. This user ID owns the Oracle database and tables and is created as an internal Oracle user only. DB2 Relational Connect does not support the use of other Oracle external authentication methods. Therefore, this user ID MUST remain an internal, Oracle-authenticated user ID. Users can change the Oracle user ID associated with the library server database after installation by running the Content Manager user mapping utility, `icmsumap` for Sun platforms. However, you must ensure that the new user ID has identical Oracle permissions to the previous user ID in use. You should not change this value once Content Manager has been installed, but instead change only the password associated with the user, unless your organization's security policy dictates otherwise.

Password (for Oracle database administration ID)
This value should not be the same value used for your library server administrator password. This is to maximize the security of your library server database and Oracle system.

Mirror directory
If you choose to use this Oracle mirroring option, it enables Oracle to

mirror the Oracle log files (useful for recovery purposes). Refer to your Oracle server documentation for more information about mirroring.

Resource manager database location
This should be the fully-qualified path name of the location where you want Oracle to store its internal database files. Additionally, this directory will be used by the installation program to generate intermediate files and database creation log files. It keeps a copy of your `icmrmdb.properties` file for future use. If you will be installing the resource manager application on an Oracle client machine, you should use `ftp` to connect to this file to your Oracle client machine (to save time and provide default values for the library server application installation). If the directory provided in this field does not exist, the installation program creates it for you. If you are using a directory that already exists, you must ensure that it is owned by the Oracle user ID and has write permissions for the Oracle user ID and Oracle group.

Resource manager host name
This is the host-only name of the Oracle server on which your resource manager database will be created. If you are installing a resource manager database, this will be the host name for the local Oracle server machine. If you are installing the resource manager application, this will be the host name for the Oracle server machine that *already* contains your resource manager database.

Chapter 26. Verifying a successful installation of Content Manager on Solaris

Use information in this section to verify a successful installation of Content Manager on an Solaris system:

Verify library server database

To verify that the library server is installed correctly:

__ 1. Check database connection by typing:

```
 # db2 connect to icmnlsdb user icmadmin using password
```

You should see output similar to the following:

```
  Database Connection Information
Database server       = DB2/SUN 7.2.4
SQL authorization ID   = ICMADMIN
Local database alias   = ICMNLSDB
```

__ 2. Check database tables by typing:

```
# db2 list tables
```

You should see several tables listed (around 127); some with names starting with ″FA″ and some starting with ″ICM″. For Oracle: you will not see any tables with names starting with ″FA″. You will only see tables with names starting with ″ICM″.

__ 3. You can also check `$ICMROOT/config/icmcrlsdb.log` and search for the term ″SQLSTATE″ to find error messages. This file may be in the **logs** directory rather than the **config** directory if the errors were detected during the installation. A few of the SQLSTATE messages are normal and you need to read the surrounding text to determine if there may have been a problem. For example, you should expect to find SQLSTATE=08003 messages in the log after the CONNECT RESET commands.

For Oracle only: Log files generated during Oracle database creation will be in the ″Library server database location″ specified during install, ending with the suffix .log. Log files generated during DB2 database creation will be in the /tmp directory, icmlscrdb.db2.log.

If database creation fails, you should verify the values used in your icmlsdb.properties file. For Oracle database creation, this file will be located in the ″Library server database location″ specified during installation. For DB2 database creation, this file will be located in the /tmp directory. If one of the values in the properties file is incorrect, you can edit the file with vi or other similar editor to correct the value. Once you are satisfied that the properties file is correct, re-run the installation program and browse to the directory where their properties file is located. You should also verify your tnsnames.ora, listener.ora, and sqlnet.ora on your Oracle server using the methods already described. The sqlnet.ora file on the Oracle client machine should use the same settings described earlier for the Oracle server.

Verify library server access modules generated

To verify that the library server access modules were generated correctly:

__ 1. Look for *.DLL files in

```
/home/db2fenc1/ICMNLSDB/DLL
```

If the DLLs are not there, then your compiler environment settings may not be set up correctly for CM. You may find some .tx3 files in the /export/home/db2fenc1/ICMNLSDB/DLL directory instead which will contain error messages.

Confirm that you are using the Forte C++ compiler Version 6.1. Make sure the ICMCOMP environment variable is set to /opt/SUNWspro/bin

If you are not picking up the SQL header files, execute the following command (as a root user) to create the symbolic links for DB2:

```
/opt/IBMdb2/V7.1/cfg/db2ln
```

After you determine the cause of the compilation problems identified in the .tx3 files, you can regenerate the access modules by executing:

```
cd /opt/IBMicm/config
java TRebuildCompTypeICM ICMNLSDB icmadmin password ICMADMIN
            /opt/IBMicm/logs/database.log
```

```
java ICMDefineSystemItemType ICMNLSDB icmadmin password
             ICMADMIN /opt/IBMicm/logs/database.log
```

__ 2. Look in the /opt/IBMicm/logs/icm81install.log to make sure you see the following output:

```
Generating DLL for access module: ICMNLSDB icmadmin ...
Number of views found: 16
Generating access module for view with ID: 200
Generating access module for view with ID: 201
Generating access module for view with ID: 202
Generating access module for view with ID: 203
Generating access module for view with ID: 204
Generating access module for view with ID: 205
Generating access module for view with ID: 206
Generating access module for view with ID: 207
Generating access module for view with ID: 208
Generating access module for view with ID: 300
Generating access module for view with ID: 301
Generating access module for view with ID: 302
Generating access module for view with ID: 303
Generating access module for view with ID: 304
Generating access module for view with ID: 400
Generating access module for view with ID: 500
All access modules rebuilt
```

This output confirms successful generation of the access module stored procedures. The access modules are used for CM item types. They are dynamically generated using the C++ compiler.

If the access modules are not correctly built, you will have problems loading documents. You will see a message in the log file (see *Messages and Codes* documentation for the name and location of the log file for the component you are using):

```
ICM7007: The access module required to access a component
table has not been built correctly. The server log contains the
name of the access module and the component type that must be
built.  Delete and re-create the item type and verify the access
module is correctly built. (STATE) : [LS RC = 7007]
com.ibm.mm.sdk.common.DKUsageError: DGL3608A: DLL not ready;
```

If you encounter this error, delete the $ICMDLL/ICMNLSDB directory (e.g. /export/home/db2fenc1/ICMNLSDB), then run `TRebuildCompTypeICM` described above.

Verify that the library server monitor program is running

To verify that the library server monitor is running, use the procedure for “Running the library server monitor program” on page 498.

Verify resource manager database

To verify that the resource manager is installed correctly:

__ 1. If you have not done so, execute the following:

```
. /export/home/db2inst1/sqllib/db2profile
```

__ 2. Check database connection by typing:

```
db2 connect to rmdb user rmadmin using password
```

You should see output similar to the following:

```
    Database Connection Information

Database server        = DB2/SUN 7.2.4
SQL authorization ID   = RMADMIN
Local database alias   = RMDB
```

__ 3. Check database tables by typing:

```
db2 list tables
```

You should see a few tables listed (around 26).

You can also check `$ICMROOT/config/icmcrrmdb.log` and search for the term ″SQLSTATE″ to find error messages. A few of the SQLSTATE messages are normal and you need to read the surrounding text to determine if there may have been a problem. For example, you should expect to find SQLSTATE=08003 messages in the log after the CONNECT RESET commands. This file may be in the logs directory rather than the config directory if the errors were detected during the installation.

Verify resource manager Web application deployment

Follow these steps to verify that the resource manager Web application is deployed correctly for either:

“Advanced Single Server Edition (AES)”

OR

“Advanced Edition (AE)” on page 398

Advanced Single Server Edition (AES)

To verify that the resource manager was deployed correctly with AES:

__ 1. Stop and restart the following services to make sure that the changes made to the HTTP Server and WAS become effective:

__ a. **Stop the HTTP Server**

```
/opt/IBMHTTPD/bin/apachectl stop
```

__ b. **Start the HTTP Server**

```
/opt/IBMHTTPD/bin/apachectl start
```

__ c. **Stop WAS Application Server**

```
/opt/WebSphere/AppServer/bin/stopServer.sh
-configFile /opt/IBMcmb/cmgmt/IDM_ICM.xml
```

OR

```
stopIDMAES.sh in /opt/CMeClient/Save/
```

(default install location on Solaris)

__ d. **Start WAS Application Server**

```
/opt/WebSphere/AppServer/bin/startServer.sh
-configFile /opt/IBMcmb/cmgmt/IDM_ICM.xml
```

OR

```
startIDMAES.sh in /opt/CMeClient/Save/
```

(default install location on Solaris)

__ 2. **Regenerate the plug-in configuration:**

__ a. Open a browser, and enter the following URL:

```
http://<hostname>:9090/admin
```

where `<hostname>` is the fully qualified host name for your WAS machine.

__ b. Configure AES:

1) Click **Configuration**.

2) Click **Open a configuration file to edit with the console**.

3) Select **Enter full path to file on server**.

4) Enter `/opt/IBMicm/cmb/cmgmt/IDM_ICM.xml`

__ c. Open up the

```
+ Nodes
   +  <hostname> (e.g. homer.stl.ibm.com)
        + Application Servers
             - Default Server
```

in the topology tree in the left pane.

In the right pane, you'll see **Application Servers: Default Server**

__ d. Under **Advanced Settings**, click **Web Server Plug-in Configuration**.

__ e. Click the **Generate** button.

__ f. After completion, you see a couple of message at the top, including:

```
New plug-in configuration has been generated.
```

Click **OK**.

__ g. Click **Configuration needs to be saved**.

__ h. Save to the following file:

```
/opt/WebSphere/AppServer/config/server-cfg.xml
```

__ i. Click **OK**

__ j. This step checks to see that the <icmrm> web application is listed in the WAS Admin Console.

Notice: icmrm is the default name and will be different if you changed it during the install.

In the WAS Admin Console, locate the Resource Manager application (icmrm)

__ k. Select **Enterprise Applications** in the topology tree in the left pane of the WAS Admin Console.

In the right pane, you will see a list of the deployed applications.

__ l. Start the Resource Manager:

__ 1) Click in the check box in front of **icmrm**

__ 2) Press the **Start** button

__ 3. **Validate the deployment:**

__ a. Look for the ICMRM web application in the WAS Admin Console.

__ b. Also check to see if the icmrm files have been copied to the WAS directory,:

```
/opt/WebSphere/AppServer/installedApps/icmrm.ear/
```

You should see output similar to the following:

```
 Auth Id  Application   Appl.     Application Id              DB    # of
          Name          Handle                                Name  Agents
-------  ------------ ----------- --------------------------- ----- ------
RMADMIN  java          35         *LOCAL.db2inst1.020627185929  RMDB    1
RMADMIN  java          36         *LOCAL.db2inst1.020627185931  RMDB    1
RMADMIN  java          37         *LOCAL.db2inst1.020627185932  RMDB    1

   Note the three java.exe processes related to RMDB.
```

If the three processes are missing, you may need to restart your icmrm Web application. If that does not help, try starting the icmrm enterprise applicatioon from the WebSphere system administration console.

Advanced Edition (AE)

To verify that the resource manager was deployed correctly with AE:

__ 1. Stop and restart the following services to make sure that the changes made to the HTTP Server and WAS become effective:

__ a. **Stop the HTTP Server**

```
/opt/IBMHTTPD/bin/apachectl stop
```

__ b. **Start the HTTP Server**

```
/opt/IBMHTTPD/bin/apachectl start
```

__ c. **Stop WAS Application Server**

```
/opt/WebSphere/AppServer/bin/wscp.sh -c "Node stop
            /Node:<node_name>/"
```

Where <node_name> is the name of the node to stop.

__ d. **Start WAS Application Server**

```
/opt/WebSphere/AppServer/bin/startupServer.sh
```

__ 2. **Regenerate the plug-in configuration**

__ a. Start the WAS Admin console:

```
/opt/WebSphere/AppServer/bin/adminclient.sh
```

__ b. Open up the

```
  - WebSphere Administrative Domain
     - Nodes
         +  <hostname> (e.g. homer.stl.ibm.com)
```

in the topology tree in the left panel.

__ c. Right click on the hostname and select **Regen Webserver Plugin** from the menu.

In the message panel at the bottom, you'll see:

```
ADGU1077I: Plugin regeneration completed successfullly...
```

__ d. In the WAS Admin Console, locate the Resource Manager application (icmrm)

(This step checks to see that the <icmrm> web application is listed in the WAS Admin Console. **Remember:** that icmrm is the default name and will be different if you changed it during the installation.)

__ e. Under your hostname, under Nodes, expand to see the **Application Servers** in the topology tree in the left pane of the WAS Admin Console.

__ f. Start the Resource Manager:

__ 1) Right mouse button click on the icmrm appserver

__ 2) From the menu, select **Start**

__ 3) In WAS AE check RM processes are running by typing:

```
# db2 list applications
```

__ 3. **Validate the deployment:**

__ a. Look for the ICMRM web application in the WAS Admin Console.

__ b. Also check to see if the icmrm files have been copied to the WAS directory, for example:

```
/opt/WebSphere/AppServer/installedApps/icmrm.ear/
```

You should see output similar to the following:

```
 Auth Id  Application   Appl.     Application Id              DB     # of
          Name          Handle                                Name  Agents
-------  ------------ ----------- --------------------------- ----- ------
RMADMIN  java          35         *LOCAL.db2inst1.020627185929  RMDB    1
RMADMIN  java          36         *LOCAL.db2inst1.020627185931  RMDB    1
RMADMIN  java          37         *LOCAL.db2inst1.020627185932  RMDB    1

   Note the three java.exe processes related to RMDB.
```

If the three processes are missing, you may need to restart your icmrm Web application. If that does not help, try starting the icmrm enterprise applicatioon from the WebSphere system administration console.

Verify resource manager Web application in a Web browser

To verify that the resource manager Web application in a Web browser:

__ 1. Start your WebSphere Application Server if it is not already started.

__ 2. Open a web browser and type in the following web addresses:

__ a. `http://<hostname>/icmrm/snoop`

Where `<hostname>` is the fully qualified hostname of your WAS machine. For example, if `homer.svl.imb.com` is your hostname, you would type:

```
http://homer.svl.imb.com/icmrm/snoop
```

You should see the snoop information, which displays network settings for your machine.

__ b. `https://<hostname>/icmrm/snoop`

You should see the snoop information again. When you type https (instead of http) you test your SSL connection.

For more information about the SSL configuration, see “Configure Secure Sockets Layer (SSL) for IBM HTTP server” on page 348.

Troubleshooting note for WAS AE: If you are unable to view the snoop information, look at the WAS configuration file to see if icmrm was deployed to a different port. This may happen if the default port is already used. View /usr/WebSphere/AppServer/config/plugin-cfg.xml. Look for information similar to:

```
<ServerGroup Name="homer/ICMRM">
        <Server CloneID="tr20agvt" Name="ICMRM">
            <Transport Hostname="homer" Port="9081" Protocol="http"/>
        </Server>
```

Notice that Port identifies **9081** (a number other than 9080), if this is the case, then add the port 9081 to your virtual host in the WAS admin console.

__ 1. Under WebSphere Administrative Domains, select **Virtual Hosts**.

__ 2. In the right pane, you see the **Hosts Alias**.

__ 3. Click **Add** to add the new port number.

Content Manager First Steps

The Content Manager First Steps program allows you to load sample data into the Content Manager servers. You perform the First Steps procedures differently depending whether you have all of the Content Manager components on one system or if you have them installed on more than one system.

For a Solaris installation of a library server or a resource manager (or both) you need to run the First Steps program from the Windows system where you installed your system administration client component. See "Running First Steps for a multiple machine Content Manager system" on page 158.

Verifying that DB2 Universal Database Relational Connect is set up correctly for Oracle

After the software is installed, a user with SYSADM authority should check the setup and create the federated database. The DB2 instance owner then configures the server to access the Oracle data sources.

Checking the federated server setup

After the federated server is setup, you can avoid potential problems by checking several key settings:

- Confirm the link between DB2 and the data source client libraries.
- Check the wrapper library file permissions.
- Ensure that the FEDERATED parameter is set to YES.

Checking the data source environment variables

When you set up the federated server, the installation process attempts to set the environment variables for the Oracle Server data sources.

Prerequisites:

A federated server that is properly setup to access your data sources. This includes the installation and configuration of any required software, such as: the client software and DB2 Relational Connect.

Procedure:

Check to make certain that the environment variables for the data sources you want access are set in the `sqllib/cfg/db2dj.ini` file.

The system administrator should check the data source environment variables.

The following table lists the valid environment variables for each data source.

Table 155. Valid data source environment variables.

Data source	Valid environment variables
Oracle	ORACLE_HOME
	ORACLE_BASE
	ORA_NLS
	TNS_ADMIN

The data source environment variables will not be set in the `sqllib/cfg/db2dj.ini` file if you:

- Install the data source client software after the DB2 federated server is setup.
- Have not installed the data source client software.

To set the environment variables:

__ 1. Install the client software (if necessary).

__ 2. Set the environment variables. The quickest way to set the data source environment variables is:
   - Run the DB2 Relational Connect installation again.

You can also manually set the environment variables.

Manually setting the Oracle environment variables

To manually set the Oracle environment variables, follow these steps:

__ 1. Edit the `db2dj.ini` file located in `sqllib/cfg` directory. The `db2dj.ini` file contains configuration information about the Oracle client software installed on your federated server. If the file does not exist, you can create a new file with this name. In the `db2dj.ini` you must specify the fully qualified path for the variable, otherwise you will encounter errors. Set the following environment variables as necessary.

ORACLE_HOME

Set the ORACLE_HOME environment variable to the directory path where the Oracle client software is installed. Specify the fully qualified path for the variable, ORACLE_HOME=<oracle_home_directory>. For example, if the Oracle home directory is `/usr/oracle/8.1.7`, the entry in the `db2dj.ini` is:

```
ORACLE_HOME=/usr/oracle/8.1.7
```

Note: If an individual user of the federated instance has the ORACLE_HOME environment variable set, federated instance does not use that setting. The federated instance uses only the value of ORACLE_HOME that you set in the DB2 profile registry.

ORACLE_BASE

ORACLE_BASE represents the root of the Oracle client directory tree. If you set the ORACLE_BASE variable when you installed the Oracle client software, set the ORACLE_BASE environment variable on the federated server. For example:

```
ORACLE_BASE=<oracle_root_directory>
```

ORA_NLS

If your system is using multiple versions of Oracle, you must ensure that:

- The appropriate ORA_NLS variable is set.
- The corresponding NLS data files for the versions you are using are available.

The location-specific data is stored in a directory specified by the ORA_NLS environment variable. For each new version of Oracle, there is a different ORA_NLS data directory.

Table 156. Oracle ORA_NLS directory name, by version.

Oracle version	Environment variable
7.2	ORA_NLS
7.3	ORA_NLS32
8.0, 8.1, 9.0.1	ORA_NLS33

For example, for federated servers that access Oracle 8.1 data sources, set the ORA_NLS environment variable:

```
ORA_NLS32=<oracle_home_directory>/ocommon/nls/admin/data>
```

TNS_ADMIN

The Oracle client expects to locate the `tnsnames.ora` file in the `/NETWORK/ADMIN` directory. The client will also look for the `tnsnames.ora` file in the `/etc` directory. If the `tnsnames.ora` file is not located in one of these directories, you need to set the TNS_ADMIN environment variable on the federated server. For example:

```
TNS_ADMIN=<tnsnames.ora_directory>
```

__ 2. Update the `.profile` file of the DB2 instance with the Oracle environment variable. You can do this by issuing the following command:

```
export PATH=$ORACLE_HOME/bin:$PATH
export ORACLE_HOME=<oracle_home_directory>
```

where `<oracle_home_directory>` is the directory where the Oracle client software is installed.

__ 3. Execute the DB2 instance `.profile` by entering:

```
. .profile
```

__ 4. Ensure that the environment variables are set on the federated server, by recycling the DB2 instance. Issue the following commands to recycle the DB2 instance:

```
db2stop
db2start
```

Confirming the link between DB2 and the data source client libraries

A federated server must be link-edited to the data source client libraries. The link-edit step is attempted when you install DB2 Relational Connect.

The link-edit step creates a wrapper library for each data source that the federated server will communicate with.

If the data source client software was not installed before you installed the DB2 server software, the link-edit step will fail. You will then need to perform the link manually.

Prerequisites:

A federated server that is properly setup to access your data sources. This includes the installation and configuration of any required software, such as: the client software, DB2 Relational Connect, or DB2 Life Sciences Data Connect.

Restrictions:

You need root authorization to run the link scripts.

Procedure:

Determine the status of the link between DB2 and the data source client libraries:

- If the link-edit was successful, the wrapper library file appears in the directory.
- If the link-edit failed, check the error message file in the directory.
- If the link-edit was not performed, neither the library file or message file appears in the directory. You will have to manually run the link script.

The following sections contain information on how to confirm the status of the link-edit, and provide instructions on how to perform the links manually.

Checking for the wrapper library files

The link-edit scripts create the wrapper libraries in specific directories, depending on the operating system. The following tables list the directory path for the library file names by data source. If the wrapper library file appears in the directory, the link-edit was successful.

The wrapper library names for Oracle are:

Table 157. Oracle wrapper library names

Operating system on your federated server	Wrapper library names for SQLNET	Wrapper library names for NET8
AIX	libdb2sqlnet.a	libdb2net8.a
Solaris	libdb2sqlnet.so	libdb2net8.so
Windows NT and Windows 2000	db2sqlnet.dll	db2net8.dll

Checking the link-edit error message files

If the link-edit fails, there will be errors listed in the error message file in the library directory. There may be an error message file in the library directory, even if the link-edit is successful. You need to open the error message file to determine if the link-edit failed. The link-edit error message file names are listed in the following table.

Table 158. Link-edit error message file names by data source

Data source	Error message file names
Oracle	djxlinkOracle.out

Manually linking DB2 to the data source client libraries

The link script creates the wrapper libraries on the federated server for the data source you are setting up. There are several reasons why the link might fail when you setup the federated server:

- If the client software is not installed before the link-edit is attempted, then the link-edit will fail.
- Check to make sure the version of the data source client is supported. The latest information is on the product Web sites. Check the DB2 Relational Connect Web sitewww.ibm.com/software/data/db2/relconnect/. If the version of the data source client you have installed is not supported, the link-edit will fail. You will have to install a client version that is supported and then perform the link manually.

You need root authorization to run the link scripts. The quickest way to link DB2 to the data source client libraries is:

__ 1. Install and configure the client software on the DB2 federated server (if necessary).

__ 2. Use the product CDs and run the DB2 Relational Connect installation again.

Alternatively, you can run the link scripts from the UNIX command prompt.

The the link script name is `djxlinkOracle`.

Issue the script from the UNIX command prompt:

```
djxlinkOracle
```

If you manually run a link script, you must issue the **db2iupdt** command on each DB2 instance to enable federated access to the data sources.

Note: There is another script, the `djxlink` script, that attempts to create a wrapper library for every data source that DB2 for UNIX and Windows supports. If you only have the client software for some of the data sources installed, you will receive an error message for each of the missing data sources when you issue the `djxlink` script.

Once the link is performed, check the permissions on the wrapper libraries after they are created. Make sure that the libraries can be read and executed by the DB2 instance owners.

Creating the federated database

After you setup the federated server, the DB2 instance owner creates a DB2 database on the federated server instance that will act as the federated database.

You can create the database two ways:

- Through the DB2 Control Center
- Through the DB2 Command Center or DB2 command line processor (CLP).

The advantage of using the DB2 Control Center is that you do not have to key in each statement and command. It is the easiest way to quickly create a database.

The steps in this section assume that you are using the DB2 Command Center or the command line processor (CLP) to create the database.

Prerequisites:

A federated server that is properly setup to access your data sources. This includes the installation and configuration of any required software, such as: the client software and DB2 Relational Connect.

Restrictions:

You need SYSADM or SYSCTRL authority to create a DB2 database.

Procedure:

Create a DB2 database on the federated server instance that will act as the federated database. For example:

```
CREATE DATABASE federated
```

This command:

- Initializes a new database.
- Creates the three initial table spaces.
- Created the system tables.
- Allocates the recovery log.

In a multi-node environment, this command affects all nodes that are listed in the `db2nodes.cfg` file. The node from which this command is issued, becomes the catalog node for the new database.

Adding Oracle data sources to a federated server

Configuring the federated server to access Oracle data sources involves supplying the server with information about the Oracle data sources and objects you want to access. You can configure access to Oracle data sources two ways:

- Through the DB2 Control Center
- Through the DB2 Command Center or command line processor (CLP)

The advantage of using the DB2 Control Center is that you do not have to key in each statement and command. It is the easiest way to quickly configure access to Oracle data sources. There are a few configuration tasks that can not be accomplished through the DB2 Control Center:

- Setting up and testing the Oracle client configuration file.
- Testing the connection to the Oracle server to validate the server definition and user mappings.
- Adding or dropping column options.

The steps in this section assume that you are using the DB2 Command Center or the command line processor (CLP) to configure access to Oracle data sources.

Prerequisites:

- A federated server and database that are setup to access Oracle data sources.
- The Oracle client software installed and configured on the federated server.
- The proper variables setup. This includes: system environment variables, db2dj.ini variables, and DB2 Profile Registry (db2set) variables.

Procedure:

To add an Oracle data source to a federated server:

1. Set up and test the Oracle client configuration file.
2. Create the wrapper.
3. Create the server definition and set the server options.
4. Create the user mappings.
5. Test the connection to the Oracle server.
6. Create nicknames for Oracle tables and views.

These steps are explained in detail in this section. Operating system-specific differences are noted where they occur.

Step 1: Set up and test a client configuration file

The client configuration file is used to connect to Oracle databases, using the client libraries that are installed on the federated server. This file specifies the location of each Oracle database server and type of connection (protocol) for the database server. The default name for the Oracle client configuration file is `tnsnames.ora`.

To set up the client configuration file, use the utility that comes with the Oracle client software. See the installation documentation from Oracle for more information about using this utility. Within the `tnsnames.ora` file, the SID is the name of the Oracle instance, and the HOST is the host name where the Oracle server is located.

The directory in which the `tnsnames.ora` file is created is `$ORACLE_HOME/network/admin` .

Test the connection to ensure that the client software is able to connect to the Oracle server. Use the Oracle **sqlplus** tool to test the connection.

Setting a different location for the tnsnames.ora file: If you decide to place the `tnsnames.ora` file in a path other than the default search path, you must set the TNS_ADMIN environment variable to specify the file location. To set this environment variable:

__ 1. Edit the `db2dj.ini` file located in the `sqllib/cfg` directory, and set the TNS_ADMIN environment variable:

```
TNS_ADMIN=x:\path\tnsnames.ora
```

__ 2. To ensure that the environment variable is set in the program, recycle the DB2 instance. Issue the following commands to recycle the DB2 instance:

```
db2stop
db2start
```

Step 2: Create the wrapper

To specify the wrapper that will be used to access Oracle data sources, use the CREATE WRAPPER statement. DB2 Relational Connect includes two wrappers for Oracle — `SQLNET` and `NET8`. To determine which wrapper to use, consult the following table.

Table 159. Oracle wrappers by client version and operating system

Oracle client	Operating system	Wrapper to use
Oracle Version 7	AIX	SQLNET
	Windows NT and Windows 2000	SQLNET
	Solaris	not applicable
Oracle Version 8	AIX	NET8
	Windows NT or Windows 2000	NET8 (recommended) or SQLNET
	Solaris	NET8

Table 159. Oracle wrappers by client version and operating system (continued)

Oracle client	Operating system	Wrapper to use
Oracle Version 9	AIX	NET8
	Windows NT or Windows 2000	NET8 (recommended) or SQLNET
	Solaris	NET8

Note: The `SQLNET` wrapper uses OCI 7 (Oracle Call Interface) API calls. The `NET8` wrapper uses OCI 8 API calls. If the Oracle 8 or Oracle 9 client is installed, you will experience better performance and functionality by using the `NET8` wrapper. Additionally, the `NET8` wrapper has LOB support. Because the OCI 7 does not support LOB data types, the `SQLNET` wrapper does not support Oracle LOB data types.

- The `SQLNET` wrapper maps Oracle LONG data types to DB2 for UNIX and Windows LOB data types.
- The `NET8` wrapper does not support Oracle LONG data types. It does map Oracle LOB data types to DB2 for UNIX and Windows LOB data types.

The following example shows the CREATE WRAPPER statement for the `NET8` wrapper:

```
CREATE WRAPPER NET8
```

Recommendation: Use the default wrapper names (SQLNET or NET8). When you create the wrapper using one of the default names, the federated server automatically picks up the default library name associated with the wrapper. If the wrapper name conflicts with an existing wrapper name in the federated database, you can substitute the default wrapper name with a name you choose. If you use a name that is different than one of the default names, you must include the LIBRARY parameter in the CREATE WRAPPER statement.

Suppose that you have a federated server running on AIX and you decide to use a wrapper name that is not one of the default names. Examples of the CREATE WRAPPER statements for `SQLNET` and `NET8` are:

```
CREATE WRAPPER mywrapper LIBRARY 'libdb2sqlnet.a'
```

```
CREATE WRAPPER mywrapper LIBRARY 'libdb2net8.a'
```

The wrapper library names for Oracle are:

Table 160. Oracle wrapper library names

Operating system on your federated server	Wrapper library names for SQLNET	Wrapper library names for NET8
AIX	libdb2sqlnet.a	libdb2net8.a

Table 160. Oracle wrapper library names (continued)

Operating system on your federated server	Wrapper library names for SQLNET	Wrapper library names for NET8
Solaris	libdb2sqlnet.so	libdb2net8.so
Windows NT and Windows 2000	db2sqlnet.dll	db2net8.dll

Step 3: Create the server definition

In the federated database, you must define each Oracle server that you want to access. You create a server definition using the CREATE SERVER statement. For example:

```
CREATE SERVER oraserver TYPE oracle VERSION 7.2 WRAPPER net8
OPTIONS (NODE 'paris_node')
```

oraserver
A name that you assign to the Oracle database server. This name must be unique. Duplicate server names are not allowed.

TYPE *oracle*
Specifies the type of data source server to which you are configuring access. The type parameter for the SQLNET and NET8 wrappers must be *oracle*.

VERSION *7.2*
The version of Oracle database server that you want to access. The supported Oracle versions are 7.x, 8.x, and 9.x.

WRAPPER *net8*
The name you specified in the CREATE WRAPPER statement.

NODE *'paris_node'*
The name of the node where the Oracle database server resides. Obtain the node name from the tnsnames.ora file.

Although the node name is specified as an option in the CREATE SERVER statement, it is required for Oracle data sources.

Locating the node name: You must define the node name in the Oracle tnsnames.ora file (see step 1). Although the *node_name* is specified as an option in the CREATE SERVER statement, it is required for Oracle data sources. This is an example of a tnsnames.ora file:

```
ORA9I.SEEL =
  (DESCRIPTION =
  (ADDRESS_LIST =
     (ADDRESS = (PROTOCOL = TCP)(HOST = somehost)(PORT = 1521)))
     (CONNECT_DATA =
     (SERVICE_NAME = ora9i.seel)))
```

The node value to use in the CREATE SERVER statement would be `ora9i.seel`.

Optional: Set additional server options: When you create the server definition, you can specify additional server options in the CREATE SERVER statement. There are general server options and data source-specific server options.

DB2 assumes that all of the Oracle VARCHAR columns contain trailing blanks. If you are certain that all VARCHAR columns in the Oracle database do not contain trailing blanks, you can set a server option to specify that the data source uses a non-blank padded VARCHAR comparison semantic. An example of the CREATE SERVER statement with this server options is:

```
CREATE SERVER oraserver TYPE oracle VERSION 7.2 WRAPPER net8
OPTIONS (NODE 'paris_node', VARCHAR_NO_TRAILING_BLANKS 'Y')
```

Use the VARCHAR_NO_TRAILING_BLANKS server option when all the columns do not contain trailing blanks. If only ssome of the VARCHAR columns do not contain trailing blanks, you can set an option on those specific columns with the CREATE NICKNAME or ALTER NICKNAME statements.

After the server definition is created, use the ALTER SERVER statement to add or drop server options.

Step 4: Create the user mappings

When you attempt to access an Oracle server, the federated server must first establish a connection to the data source. The federated server does this by using a valid user ID and password to that data source. You must define an association between the federated server user ID and password and the data source user ID and password. This association must be created for each user ID that will be using the federated system to send distributed requests. This association is called a *user mapping*.

Use the CREATE USER MAPPING statement to map the local user ID to the Oracle server user ID and password; for example:

```
CREATE USER MAPPING FOR robert SERVER oraserver
OPTIONS (REMOTE_AUTHID 'rob', REMOTE_PASSWORD 'then4now')
```

robert The local user ID that you are mapping to a user ID defined at an Oracle server.

SERVER *oraserver*
The name of the Oracle server that you defined in the CREATE SERVER statement.

REMOTE_AUTHID *'rob'*
Tthe user ID at the Oracle database server to which you are mapping

robert. This value is case sensitive unless you set the FOLD_ID server option to ’U’ or ’L’ in the CREATE SERVER statement.

REMOTE_PASSWORD *’then4now’*
The password associated with *’rob’*. This value is case sensitive unless you set the FOLD_PW server option to ’U’ or ’L’ in the CREATE SERVER statement.

You can use the DB2 special register **USER** to map the authorization ID of the person issuing the CREATE USER MAPPING statement to the data source authorization ID specified in the **REMOTE_AUTHID** user option. The following is an example of the CREATE USER MAPPING statement which includes the **USER** special register:

```
CREATE USER MAPPING FOR USER SERVER oraserver
OPTIONS (REMOTE_AUTHID 'rob', REMOTE_PASSWORD 'then4now')
```

Restriction: The user ID at the Oracle data source must have been created using the Oracle create user command with the ’identified by’ clause, instead of the ’identified externally’ clause.

Step 5: Test the connection to the Oracle server

Test the connection to the Oracle server to ensure that you can establish a connection, using the server definition and user mappings you defined. Open a pass-through session and issue a SELECT statement against the Oracle system tables. For example:

```
SET PASSTHRU server_name
SELECT count(*) FROM sys.all_tables
SET PASSTHRU RESET
```

If the SELECT returns a count, then your server definition and user mapping are set up properly. If the SELECT returns an error, you might have to:

- Check the Oracle server to make sure that it is configured for incoming connections.
- Check your user mapping to make sure that the settings for the REMOTE_AUTHID and REMOTE_PASSWORD options are valid for connections to the Oracle server.
- Check the Oracle client software on the DB2 federated server to make sure that it is installed and configured correctly to connect to the Oracle server.
- Check your DB2 federated variables to make sure that they are correct for working with the Oracle server. This includes checking the system environment variables, db2dj.ini variables, and the DB2 Profile Registry (db2set) variable.
- Check your server definition and possibly drop it and create it again.
- Check your user mapping and possibly alter it or create another if necessary.

Step 6: Create the nicknames for tables and views

The federated database relies on catalog statistics for nicknamed objects to optimize query processing. These statistics are gathered when you create a nickname for a data source object using the CREATE NICKNAME statement. The federated database verifies the presence of the object at the data source, and then attempts to gather existing data source statistical data. Information useful to the optimizer is read from the data source catalogs and put into the global catalog on the federated server. Because some or all of the data source catalog information might be used by the optimizer, update statistics (using the data source command equivalent to RUNSTATS) at the data source before you create a nickname.

For each Oracle server you defined, assign a nickname to each table or view you want to access on those servers. You will use these nicknames, instead of the names of the data source objects, when you query the Oracle servers. Nicknames can be up to 128 characters in length.

The federated server will fold the Oracle server, schema, and table names to uppercase unless you enclose them in double quotation marks (″). The following example shows a CREATE NICKNAME statement:

```
CREATE NICKNAME PARISINV FOR oraserver."france"."inventory"
```

:

PARISINV

A unique nickname used to identify the Oracle table or view.

Note: the nickname is a two-part name—the schema and the nickname. If you omit the schema when creating the nickname, the schema of the nickname will be the authorization ID of the user creating the nickname.

oraserver."france"."inventory"

A three-part identifier for the remote object:

- *oraserver* is the name you assigned to the Oracle database server in the CREATE SERVER statement.
- *france* is the name of the remote schema to which the table or view belongs.
- *inventory* is the name of the remote table or view that you want to access.

Repeat this step for each Oracle table or view for which you want create nicknames. When you create the nickname, DB2 will use the connection to query the data source catalog. This query tests your connection to the data source using the nickname. If the connection does not work, you will receive an error message.

Tuning and troubleshooting the configuration to Oracle data sources

After you have set up the configuration to Oracle data sources, you may want to modify the configuration to improve performance. For example, you might want to set the DB2_DJ_COMM environment variable to improve performance when the Oracle data source is accessed.

Improving performance by setting the DB2_DJ_COMM environment variable

If you find that it takes an inordinate amount of time to access the Oracle server, you can improve the performance by setting the DB2_DJ_COMM environment variable. Setting the DB2_DJ_COMM environment variable will load the wrapper when the federated server initializes rather than when you attempt to access the data source.

__ 1. Set the DB2_DJ_COMM environment variable to the wrapper library that corresponds to the wrapper that you specified. Suppose that your federated server is running AIX and the wrapper you are using is NET8. The command to set the DB2_DJ_COMM environment variable is:

```
db2db2set DB2_DJ_COMM= 'libdb2net8.a'
```

Consult the following table for the proper library name.

Table 161. Oracle wrapper library names

Operating system on your federated server	SQLNET wrapper library names	NET8 wrapper library names
AIX	libdb2sqlnet.a	libdb2net8.a
Solaris	libdb2sqlnet.so	libdb2net8.so

__ 2. Recycle the DB2 instance to ensure that the environment variables are set in the program. When you recycle the instance, the DB2 instance accepts the changes that you made. Issue the following commands to recycle the DB2 instance:

```
db2stop
db2start
```

Connectivity problems

For each HOST in the DESCRIPTION section of the `tnsnames.ora` file, you might need to update the `hosts` file:

```
/etc/hosts
```

Whether you update this file depends on how TCP/IP is configured on your network. Part of the network must translate the remote host name specified in the DESCRIPTION section in the `tnsnames.ora` file to an address. If your network has a named server that recognizes the host name, you do not need to update the TCP/IP `hosts` file. Otherwise, you need an entry for the remote host. See your network administrator to determine how your network is configured.

Chapter 27. Installing Enterprise Information Portal components on Solaris

The EIP components are installed on Solaris using a command-line installation program named `cmbsuninst.sh`. The program offers six options:

1. Install and configure
2. Install only
3. Uninstall
4. Configure
5. List installed components
6. Quit

Table 162 provides the EIP component installation package names and descriptions. The Uninstall base package and Development Toolkit Base package are installed with all component packages.

Table 162. EIP installation packages

Package	Description
`application cmbcomub`	Content Manager EIP Version 8.2 Uninstall Base
`application cmbcomdtb`	Content Manager EIP Version 8.2 Development Toolkit Base
`1: application cmbfedc`	Content Manager EIP Version 8.2 Federated connector
`2: application cmbrdbc`	Content Manager EIP Version 8.2 Relational Database connector
`3: application cmbdlc`	Content Manager EIP Version 8.2 CM V7 connector
`4: application cmbodc`	Content Manager EIP Version 8.2 OnDemand connector
`5: application cmbip390c`	Content Manager EIP Version 8.2 ImagePlus for OS/390 connector
`6: application cmbas400c`	Content Manager EIP Version 8.2 AS/400 connector
`7: application cmbddc`	Content Manager EIP Version 8.2 Domino .Doc connector
`8: application cmbesc`	Content Manager EIP Version 8.2 Extended Search connector
`9: application cmbicc`	Content Manager EIP Version 8.2 Information Catalog connector
`10: application cmbcmc`	Content Manager EIP Version 8.2 Content Manager Version 8 connector
`11: application cmbgcs`	IBM Web Crawler

Table 162. EIP installation packages (continued)

Package	Description
`12: application cmbikfsv`	Content Manager EIP Version 8.2 Information Mining
`13: application cmbic`	Content Manager EIP Version 8.2 Information Center
`14: application cmbdb`	Content Manager EIP Version 8.2 system administration database

Installing EIP component packages

Before you begin to install EIP, be sure to perform all the tasks listed in Chapter 24, "Performing pre-installation steps on Solaris", on page 345.

To start the installation program, `cd` to the installation directory and type `./cmbsuninst.sh` at a command prompt. The program checks to see if the DISPLAY environmental variable is set. You will be presented with a license agreement GUI interface. Select **ACCEPT** to continue the installation or **DECLINE** to exit. **Requirement:** You must export the display to your local system to install EIP, because the license agreement is a GUI panel.

If the prerequisites are located, the program displays six installation options:

1. Install and configure
2. Install only
3. Uninstall
4. Configure
5. List installed components
6. Quit

Type an installation option number and follow system prompts. The default option is `1. Install and configure`.

1. Install and configure

When you type `1. Install and Configure` the program prompts you to select the installation and configuration type:

1. Install and configure all components.
2. Install and configure selected components.
3. Restart
4. Quit

Type `1` or `2` to begin installing and configuring EIP component packages.

The program displays the component installation packages in Table 162 on page 417. If you select installation option `2. Install and configure selected components`, the program provides an input line to enter the corresponding numbers of the packages to be installed and configured. Use spaces or commas to separate the package numbers.

Follow system prompts to verify and accept all or selected component packages. The program installs packages to the server without user input. The program does prompt you for configuration information.

If all packages are installed and configured without errors, the installation was successful. If the installation fails, the program notifies you, uninstalls selected packages and sends the output to a log file.

The program writes all installation and uninstallation information to a console and also to a log file in `/tmp/cmb/cmbinst.log`

2. Install Only

When you select `2. Install Only` the program prompts you to select the installation type:

1. Install all components.
2. Install selected components.
3. Restart
4. Quit

Type `1` or `2` to begin installing EIP component packages. The program displays the component installation packages in Table 162 on page 417. If you selected option `2`, the program provides an input line to enter the corresponding numbers of the packages to install. Use spaces or commas to separate the package numbers.

Follow system prompts to verify and accept all or selected component packages. The program adds packages to the server without any user input.

If the packages are installed without errors, the installation was successful. If the installation fails, it will continue to install until all selected components are attempted. and sends the output to a log file. The program writes all installation information to a console and also to a log file in `/tmp/cmb/cmbuninst.log`.

3. Uninstall

When you select option 3, Uninstall, the program prompts you to select the uninstallation type.

1. Uninstall all components
2. Uninstall selected components

3. Restart
4. Quit

Type 1 or 2 to begin uninstalling EIP component packages. If you select option 2, the program provides an input line to enter the corresponding numbers of the packages to uninstall. Use spaces or commas to separate the package numbers.

If uninstallation of any selected components fails, the program continues to uninstall until all selected components are attempted.

4. Configure

When you select option 4, Configure, the program prompts you to select the configuration type:

1. Configure all components.
2. Configure selected components.
3. Restart
4. Quit

Type 1 or 2 to begin configuration of the installed components. The configuration program requires user input.

When configuration is complete, the program displays Configuration Completed and prompts you to check the log file for possible errors: `/tmp/cmb/cmbinst.log`

5. List installed components

The installation program displays all EIP components and places an asterisk next to the components already installed. The program then exits.

6. Quit

The installation program exits when you select option 6.

Exporting classpath, environment variables on Solaris

You must use a configuration program that exports classpath, environment variables and other information before you can use EIP.

1. cd to `/opt/IBMcmb/bin`
2. Type `. ./cmbenv81.sh`

Verifying EIP installation

See Chapter 28, “Verifying a successful installation of Enterprise Information Portal on Solaris”, on page 421.

Chapter 28. Verifying a successful installation of Enterprise Information Portal on Solaris

Use information in this section to verify a successful installation of Enterprise Information Portal on a Solaris system. It includes the following procedures:

- "Enterprise Information Portal First Steps"
- "Verify Enterprise Information Portal system administration database"
- "Verify system administration database and system administration client communication" on page 422
- "Run low-level connection tests" on page 422
- "Verify Enterprise Information Portal connection to Content Manager Version 8" on page 424

Enterprise Information Portal First Steps

The Enterprise Information Portal First Steps program allows you to load sample data into the Enterprise Information Portal system administration database. You perform the First Steps procedures differently depending whether you have all of your Enterprise Information Portal components installed on one system or if you have them installed on more than one system.

For a Solaris installation of the system administration database, you need to run the First Steps program from the Windows system where you installed your system administration client component. See "Running First Steps with Enterprise Information Portal components installed on multiple machines" on page 196.

Verify Enterprise Information Portal system administration database

To verify that the Enterprise Information Portal system administration database is installed correctly:

__ 1. Check database connection by typing:

```
$ db2 connect to icmnlsdb user icmadmin using password
```

You should see output similar to the following:

```
Database Connection Information

Database server        = DB2/SUN 7.2.4
SQL authorization ID   = ICMADMIN
Local database alias   = ICMNLSDB
```

__ 2. Check database tables by typing:

```
$ db2 list tables
```

You should see several tables listed (around 125); some with names starting with ″FA″ and some starting with ″ICM″.

Verify system administration database and system administration client communication

Because there is no administration client on Solaris, you must configure a connection between the Windows administration client and the Solaris databases. There are two ways to connect an administration client to a remote database:

- Connect through an RMI server (see Chapter 33, “Configuring an RMI server”, on page 507).
- Define a connection by following the steps in “Connecting the administration client to a remote administration database” on page 447

Run low-level connection tests

Verify that the Enterprise Information Portal federated connector and the Content Manager Version 8 connector are installed correctly, run the indicated sample programs in this section.

Before you run the tests

Before you run the connection tests:

__ 1. It is important that any user ID that is used for EIP application development work must be a member of the group that your db2 instance user ID belongs to, for example: **db2iadm1** (the group that db2inst1 belongs to).

__ 2. Login as **icmadmin**. Perform the following setup to run the EIP sample programs. Copy the java samples to a local directory eipsamps off of your home directory:

```
 $  cp -R /opt/IBMcmb/samples/java $HOME/eipsamps
```

This also changes the ownership of the files to the current user.

__ 3. Ensure you have the proper Enterprise Information Portal development environment. It is recommended that you add these two lines to the `.profile` of the users doing EIP application development work. Note the space between the period (.) and the first slash (/):

__ a. Establish the DB2 environment.

```
$ . /export/home/db2inst1/sqllib/db2profile
```

__ b. Establish the EIP development environment.

```
$ . /opt/IBMcmb/bin/cmbenv81.sh
```

Running the connection tests

Run the following two tests:

__ 1. **Federated connector test:**

```
$ cd $HOME/eipsamps/java/fed
$ javac TConnectFed.java
$ java TConnectFed icmnlsdb icmadmin password
```

Expected output:

```
$ java TConnectFed icmnlsdb icmadmin password
*** connecting to datastore : icmnlsdb
*** datastore connected ***
user icmadmin dsName icmnlsdb
datastore disconnected
user icmadmin dsName icmnlsdb
```

__ 2. **Content Manager V8 connector test:**

```
$  cd $HOME/eipsamps/java/icm
$  javac SConnectDisconnectICM.java
$  java SConnectDisconnectICM icmnlsdb icmadmin password
```

Expected output:

```
$ java SConnectDisconnectICM icmnlsdb icmadmin password
======================================
IBM Enterprise Information Portal v8
Sample Program:  SConnectDisconnectICM
--------------------------------------
Database: icmnlsdb
UserName: icmadmin
======================================
Connecting to datastore (Database 'icmnlsdb', UserName
         'icmadmin')...
Connected to datastore (Database 'icmnlsdb', UserName
         'icmadmin').
Disconnecting from datastore & destroying reference...
Disconnected from datastore & destroying reference.
==========================================
Sample program completed.
==========================================
```

If you get the following type errors:

```
TConnectFed.java:33: package com.ibm.mm.sdk.common does not
                                                  exist
import com.ibm.mm.sdk.common.*;
^
```

You forgot to establish the EIP development environment. Note the space between the period (.) and the first slash (/) in the command.

Execute:

```
$ . /opt/IBMcmb/bin/cmbenv81.sh
```

Verify Enterprise Information Portal connection to Content Manager Version 8

To verify the connection from Enterprise Information Portal to Content Manager:

__ 1. On your Windows system, start the Enterprise Information Portal system administration client, as follows: Administration Client on Windows:

Start -> Programs -> Enterprise Information Portal V8.2 -> Administration

__ 2. On the left-hand side of the window, right-click on **Servers** and select **New**.

__ 3. From the list, select **Content Manager v8**.

__ 4. Enter the connection information:

Server Name: ICMNLSDB

__ 5. Click on the **Test Connection** button.

__ 6. You should see that the connection is successful.

Chapter 29. Installing Content Manager eClient on Solaris

After you have verified your Enterprise Information Portal installation, you can install the eClient.

If you are installing the eClient on the same machine that you installed Enterprise Information Portal, you do not need to install any additional prerequisites.

Before you install the eClient

Before you begin the installation process for the eClient, here are some things to consider:

If you are using WebSphere Application Server (WAS) AES, stop any server that is already running on WAS. However, if you are using WAS AE, make sure that the WebSphere Application Server administration server (AE) is running before starting the eClient installation.

If you are using WebSphere Application Server Version 5, make sure that you have started the application server. To start the application server:

1. Change to `*WASROOT*/bin` subdirectory, where *WASROOT* is the root directory where WebSphere is installed.
2. Execute

   ```
   ./startServer.sh server1
   ```

Installing the eClient

To install the eClient on your application server on Sun Solaris:

1. Insert the eClient CD into the CD drive.
2. **Optional:** If you are installing on Sun Solaris using an X window session (for example, Exceed), enter this command:

   ```
   export DISPLAY=hostname:0.0
   ```

   where `hostname` is the host name or IP address where you want to be able to view the install panels.
3. From the launchpad directory, enter this Java command to manually run the launchpad:

   ```
   java com.ibm.cm.install.launchpad.LaunchPad
   ```

   Note: You must have root or sudo privileges to run the launchpad.

4. Follow the instructions in the installation windows. The default directory to install the eClient is `/opt/CMeClient`.
5. If you are connecting to Content Manager Version 8, the default local file location of the data server list file is `/opt/ibm/cmb/cmgmt/cmbicmsrvs.ini`

   After you install the eClient files, the installation program checks for WebSphere Application Server (WAS). If the installation program detects WAS, you can continue with the automatic configuration of the Web application for the eClient. You can choose to exit without automatically configuring the application with WebSphere.
6. Start the eClient on WebSphere. To start the eClient on WebSphere:
   a. Change to the `/Save` subdirectory.
   b. For WebSphere 4.0.5 AE, enter `startIDMAE.sh`; for WebSphere 4.0.5 AES, enter `startIDMAES.sh`; for WebSphere 5, enter `startIDMServer.sh`.

   To stop the eClient, enter `stopIDMAE.sh` or `stopIDMAES.sh`.
7. **Optional:** If you choose not to perform the automatic configuration, you must set up and configure the eClient as a Web application.

Validating the eClient installation

Follow these steps to validate that the eClient is installed correctly:

For WebSphere AES

__ 1. After installation has completed, if you are using WebSphere AES, you need to start the server:

```
$ /opt/WebSphere/AppServer/bin/startServer.sh
```

__ 2. Execute the utility to start the eClient in WebSphere:

```
/opt/CMeClient/Save/startIDMAES.sh
```

__ 3. Before starting the eClient, start the WebSphere Admin console to confirm that the eClient Application Server has been created. Start it if necessary.

__ 4. In your browser, enter:

```
http://<hostname>/eClient81/IDMInit
```

The eClient login page should open.

For WebSphere AE

__ 1. Execute the utility to start the eClient in WebSphere:

```
/opt/CMeClient/Save/startIDMAE.sh
```

__ 2. Before starting the eClient, start the WebSphere Admin console to confirm that the eClient Application Server has been created. Start it if necessary.

__ 3. In your browser, enter:

```
http://<hostname>/eClient81/IDMInit
```

The eClient login page should open.

If you installed the eClient correctly and the address is correct, the Logon window should open.

If you configured the eClient correctly, you should be able to access the content servers that you defined. The content servers that the eClient supports include:

- IBM Content Manager for Multiplatforms Version 7.1
- IBM Content Manager for Multiplatforms Version 8.1
- IBM Content Manager for Multiplatforms Version 8.2
- IBM Content Manager OnDemand for Multiplatforms Version 7.1
- IBM Content Manager OnDemand for OS/390 Version 2.1
- IBM Content Manager OnDemand for OS/390 Version 7.1
- IBM Content Manager OnDemand for iSeries Version 4.5
- IBM Content Manager OnDemand for iSeries Version 5.1
- IBM Content Manager ImagePlus for OS/390 Version 3.1
- IBM VisualInfo for AS/400 Version 4.3 or Version 5.1

Part 5. After-installation configuration and setup procedures

This section contains the procedures that occur after Content Manager has been installed:

- Chapter 30, “Installing and Configuring Tivoli Storage Manager (TSM)”, on page 431
- Chapter 31, “Configuring Enterprise Information Portal components”, on page 447
- Chapter 32, “Using Content Manager after-install programs and procedures”, on page 481
- Chapter 33, “Configuring an RMI server”, on page 507
- Chapter 34, “Generating configuration files”, on page 515

Chapter 30. Installing and Configuring Tivoli Storage Manager (TSM)

This section describes each step required to set up Tivoli Storage Manager (TSM) on Content Manager for Windows, AIX, and Solaris.

The Tivoli Storage Manager (TSM) can be used with Content Manager resource managers on AIX, Solaris, and Windows to store objects on TSM supported devices. (TSM supported devices include optical libraries and tape media.) The use of TSM is optional and is needed only if you want to provide long-term storage for your objects on devices other than the fixed disks attached to the resource manager. This section includes the following topics:

- Defining TSM media and associated policies for use by the resource manager
- Defining a TSM node for each resource manager
- Configuring the TSM API client option files on the resource manager machine
- Configuring the resource manager to use TSM
- Configuring the TSM Server and the API client to support the resource manager
- Customizing the resource manager to use specific TSM management classes
- Determining the space available in TSM
- Using overflow storage systems
- Troubleshooting for the resource manager and TSM

Prerequisite information

Tivoli Storage Manager (TSM), Version 4.2.1 or later is required for use on Content Manager, Version 8.

Configuration requirements

The resource manager uses the local TSM API client to store objects into the TSM Server. The TSM server is managed and administered independently of the resource manager. The TSM administrator must ensure that the following conditions are met:

- All the normal requirements for TSM storage are monitored and managed accordingly
- All required TSM policies, management classes, storage pools, and volumes are defined accordingly
- All required TSM storage pools and volumes are online

- All TSM storage pools and volumes have sufficient storage space to satisfy the needs of the client resource managers
- The TSM Server is active when the resource manager needs to read from or write to its storage repository

If your TSM configuration cannot support the resource manager, system requests (that require TSM services) will fail. The TSM administrator should examine the system to ensure that it will support the storage and retrieval of objects by Content Manager.

Step 1. Defining TSM media and associated policies for use by the resource manager

There are a number of definition commands on the TSM server that must be executed to provide support for the Content Manager resource manager. You can use either the TSM Web administrator console or the command line method to enter commands.

Refer to the *Tivoli Storage Manager Administrator's Guide* for TSM basics and to the *Tivoli Storage Manager Administrator's Reference* to understand the structure and function of the Administrator Commands.

TSM Server definitions

The following sequence of definitions on the TSM Server are provided in the TSM administrator command format:

DEFINE DOMAIN (Define a new Policy Domain)

Use this command to define a new policy domain. A policy domain contains policy sets, management classes, and copy groups. A client is assigned to one policy domain. The ACTIVE policy set in the policy domain determines the rules for clients assigned to the domain. The rules control the archive, backup, and space management services provided for the clients.

You must activate a policy set in the domain before clients assigned to the policy domain can back up, archive, or migrate files.

Important: Set up to ensure that the primary copy of any file cannot be deleted as a result of the policies in TSM. (The only way to delete objects should be through the Content Manager resource manager.)

DEFINE POLICYSET (Define a new Policy Set)

Use this command to define a policy set in a policy domain. A policy set contains management classes, which contain copy groups. You can define one or more policy sets for each policy domain.

DEFINE STGPOOL (Define a Storage Pool)

Use this command to define a primary storage pool or a copy storage pool. You use a primary storage pool as the destination for backup files, archive files, or files migrated from client nodes. You use a copy storage pool to store backup copies of files that are in primary storage pools.

DEFINE MGMTCLASS (Define a Management Class)
Use this command to define a new management class in a policy set. Use names that can be easily associated with the type of storage pool media in the backup copy group associated with this management class. For example, if your `COPY` Destination is to a Disk Storage Pool, you might call the management class `DISK`. This method of associating names to the storage pool will help you configure your resource manager to move data to select TSM media pools.

DEFINE COPYGROUP — Backup
Use this command to define a new backup copy group within a specific management class, policy set, and policy domain.

ASSIGN DEFMGMTCLASS (Assign a Default Management Class)
Use this command to specify a management class as the default management class for a policy set. You must assign a default management class for a policy set before you can activate that policy set. To ensure clients can always back up and archive files, choose a default management class that contains both an archive copy group and a backup copy group. The server uses the default management class to manage client files when a management class is not otherwise assigned or appropriate. For example, the server uses the default management class when a user does not specify a management class in the include-exclude list. See the Administrator's Guide for details.

VALIDATE POLICYSET (Verify a Policy Set)
Use this command to verify that a policy set is complete and valid before you activate it. The command examines the management class and copy group definitions in the policy set and reports on conditions that you need to consider before activating the policy set.

ACTIVATE POLICYSET (Activate a New Policy Set)
Use this command to copy the contents of a policy set to the ACTIVE policy set for the domain. The server uses the rules in the ACTIVE policy set to manage client operations in the domain. You can define multiple policy sets for a policy domain, but only one policy set can be active. The current ACTIVE policy set is replaced by the one you specify when you issue this command. You can modify the ACTIVE policy set only by activating another policy set.

REGISTER NODE (Register a Client Node)
Use this command to register a client node to the server. This command also automatically creates an administrative user ID with client owner authority over the node. You can use this administrative user ID to access the Web backup-archive client from remote locations

through a Web browser. If an administrative user ID already exists with the same name as the node being registered, an administrative user ID is not automatically defined. The client node is registered without an administrative user ID. This process also applies if your site uses open registration. If a client requires a different policy domain than STANDARD, you must register the client node with this command or update the registered node.

Example

Here is an example showing one possible way to enter the setup definition and activate commands. Understand your needs for your own application, then use this example as a guide to understanding which parameters you might need to set for specific commands:

```
//DEFINE DOMAIN
define domain CMDomain Description='Content Manager Domain' backretention=60
                       archretention=365
//DEFINE POLICYSET
define policyset CMDomain CMPolicy Description='Content Manager Policy Set'
//DEFINE A STORAGE POOL
define stgpool CMDiskPool disk pooltype=primary
               description='Content Manager Disk Storage Pool'
               access=readwrite maxsize=nolimit nextstgpool=''
//DEFINE THE MANAGEMENT CLASS
define mgmtclass CMDomain CMPolicy Disk
                 description='Content Manager TSM Managment Class'
//DEFINE THE COPYGROUP
define copygroup CMDomain CMPolicy Disk destination=CMDiskPool
                 verdeleted=1 retextra=3 retonly=45 mode=absolute
                 serialization=shrstatic
//ASSIGN A DEFAULT MANAGEMENT CLASS
assign defmgmtclass CMDomain CMPolicy Disk
//VERIFY A POLICY SET
validate policyset CMDomain CMPolicy
//ACTIVATE A NEW POLICY SET
activate policyset CMDomain CMPolicy
```

Step 2. Defining a TSM node for each resource manager

To define the resource manager’s node as a TSM client node, the TSM administrator must register the resource manager’s NodeName as a TSM client node with the Policy Domain you’ve selected for the Content Manager resource manager. Specify parameters as follows:

- REGister Node *nodename password*
- CONtact = *contactinfo*
- DOmain = *domainname*
- COMpression = Client
- ARCHDELete = Yes
- BACKDELete = Yes

Example using a TSM administrator command:

```
//DEFINE A CM resource manager AS A NODE FOR TSM
                (for example, icmrmaix)
register node <node_name> <password> contact=<user@somewhere.com>

//example using real data:
register node icmrm cm4you contact=P.Sanchez, CM Admin.
                domain=CMDomain backdelete=yes
```

See the **REGISTER NODE** command in the *Tivoli Storage Manager Administrator's Reference*.

Step 3. Customizing TSM API client files on the resource manager machine

Here are some things that you need to know to configure the resource manager to use TSM:

1. You need to have a TSM client installed, then you must configure a TSM API client option file.
2. For performance and reliability reasons, you should configure the resource manager to use the TSM API Passwordaccess PROMPT.
3. The TSM API Access method GENERATE is supported, but the resource manager first attempts to access TSM with PROMPT. If the PROMPT is not successful, it retries, using GENERATE. **Remember this hint:** If you use GENERATE, you need to use the TSM API sample program `dapismp` to change the password, which in turn, enables this feature.

For the following example, there is a single TSM server on an AIX machine with hostname NATHAN, and four resource managers as shown in Table 163.

Table 163. Example TSM configuration

Resource manager database name	Resource manager application name	Platform	Hostname	TSM nodename	TSM API options file
RMAIX	icmrm	AIX	NATHAN	icmrmaix	icmrmaix.opt
RMSOL	icmrm	Solaris	CHILI	icmrmsol	icmrmsol.opt
RMWN1	icmrm	Windows 2000	BADAL1	icmrmwn1	icmrmwn1.opt
RMWN2	icmrm	Windows 2000	ERIN	icmrmwn2	icmrmwn2.opt

Each resource manager needs to have a TSM API client options file configured locally, and an `icmrm.properties` file.

Sample TSM option files

This section shows sample TSM options files for Unix (AIX/Solaris) platform machines and for Windows machines.

- AIX/Solaris examples include one option file and one system file.
- Windows examples include only one option file.
- For all platforms, consider using the TSM API `include` parameter to distinguish which TSM Management class is being used to store data.

Adjust file names and paths according to your system's configuration.

TSM API options file for resource manager RMAIX on AIX machine NATHAN (icmrmaix.opt)

```
************************************************************************
* Tivoli Storage Manager
*
*
*
* Sample Client User Options file for AIX and SunOS (dsm.opt.smp)
*
************************************************************************
*  server to contact if more than one is defined in your client
*  system options file (dsm.sys).  Copy dsm.opt.smp to dsm.opt.
*  If you enter a server name for the option below, remove the
*  leading asterisk (*).
************************************************************************
*SErvername       A server name defined in the dsm.sys file
*TRACEFL                 INSTR_CLIENT_DETAIL FS API PID COMM SESSION
*TRACEFIL FS API PID SESSION      /home/icmrm/log/tsmapi.log
SErvername nathan
```

TSM system options file for resource manager RMAIX on AIX machine NATHAN (dsm.sys)

```
************************************************************************
* Tivoli Storage Manager
*
*
*
* Sample Client User Options file for AIX and SunOS (dsm.sys.smp)
*
************************************************************************
*  This file contains the minimum options required to get started
*  using TSM.  Copy dsm.sys.smp to dsm.sys.  In the dsm.sys file,
*  enter the appropriate values for each option listed below and
*  remove the leading asterisk (*) for each one.
*  If your client node communicates with multiple TSM servers, be
*  sure to add a stanza, beginning with the SERVERNAME option, for
*  each additional server.
************************************************************************
SErvername  nathan
   COMMmethod       TCPip
   TCPPort          1500
   TCPServeraddress  nathan.svl.ibm.com
   Nodename          icmrmaix
   Passwordaccess    PROMPT
   Inclexcl          /home/icmadmin/TSMmc.inc
```

TSM include file for resource manager RMAIX on AIX machine NATHAN (TSMmc.inc)

This example shows what is required if you need to use TSM Management classes for the node other than the Default Management class:

```
TSMmc.inc
//The following is only required if you did not define a policy set for the
//Object server to use.
  include          DISK* DISK
```

TSM API options file for resource manager RMSOL on Solaris machine CHILI (icmrmsol.opt)

```
************************************************************************
* Tivoli Storage Manager
*
*
*
* Sample Client User Options file for AIX and SunOS (dsm.opt.smp)
*
************************************************************************
*  server to contact if more than one is defined in your client
*  system options file (dsm.sys).  Copy dsm.opt.smp to dsm.opt.
*  If you enter a server name for the option below, remove the
*  leading asterisk (*).
************************************************************************
*SErvername       A server name defined in the dsm.sys file
*TRACEFL                 INSTR_CLIENT_DETAIL FS API PID COMM SESSION
*TRACEFIL FS API PID SESSION      /home/icmrm/log/tsmapi.log
SErvername nathan
```

TSM API options file for resource manager RMSOL on Solaris machine CHLI (dsm.sys)

```
************************************************************************
* Tivoli Storage Manager
*
*
*
* Sample Client User Options file for AIX and SunOS (dsm.sys.smp)
*
************************************************************************
*  This file contains the minimum options required to get started
*  using TSM.  Copy dsm.sys.smp to dsm.sys.  In the dsm.sys file,
*  enter the appropriate values for each option listed below and
*  remove the leading asterisk (*) for each one.
*  If your client node communicates with multiple TSM servers, be
*  sure to add a stanza, beginning with the SERVERNAME option, for
*  each additional server.
************************************************************************
SErvername  nathan
   COMMmethod        TCPip
   TCPPort           1500
   TCPServeraddress  nathan.svl.ibm.com
   Nodename          icmrmaix
   Passwordaccess    PROMPT
   Inclexcl          /home/icmadmin/TSMmc.inc
```

TSM API options file for resource manager RMWN1 on Windows machine BADAL1 (icmrmwn1.opt)

```
*********************************************************************
* Tivoli Storage Manager
*
* Sample dsm.opt for the Microsoft Windows Backup-Archive Client
*********************************************************************
*TRACEFL         INSTR_CLIENT_DETAIL FS API PID COMM SESSION
*TRACEFIL        e:\%FRNROOT%\log\TSM.log
*====================================================================
* TCP/IP
*====================================================================
commmethod      tcpip
tcpport          1500
TCPServeraddress nathan
Include          ?:DISK*DISK
NODEname         icmrmwn1
NamedPipe        \\ntmachine\pipe\TSMpipe
PasswordAccess   Prompt
```

TSM API options file for resource manager RMWN2 on Windows machine ERIN1 (icmrmwn2.opt)

```
*********************************************************************
* Tivoli Storage Manager
*
* Sample dsm.opt for the Microsoft Windows Backup-Archive Client
*********************************************************************
*TRACEFL         INSTR_CLIENT_DETAIL FS API PID COMM SESSION
*TRACEFIL        e:\%FRNROOT%\log\TSM.log
*====================================================================
* TCP/IP
*====================================================================
commmethod      tcpip
tcpport          1500
TCPServeraddress nathan
Include          ?:DISK*DISK
NODEname         icmrmwn2
NamedPipe        \\ntmachine\pipe\TSMpipe
PasswordAccess   Prompt
```

Step 4. Configuring the resource manager to use TSM

To configure the resource manager to use TSM, you need to do the following:

1. Ensure that you have properly configured the TSM API client as shown by the examples in “Step 3. Customizing TSM API client files on the resource manager machine” on page 435.

2. “Configure the resource manager properties file”.
3. Start the resource manager and “Configure the resource manager using the Content Manager system administration client” on page 440.

Configure the resource manager properties file

If you installed the Content Manager resource manager with WebSphere using the default values and locations, you can find the ICMRM.properties file in the following location:

On Windows:

```
c:\WebSphere\AppServer\installedApps\icmrm.ear
\icmrm.war\WEB-INF\classes\com\ibm\mm\icmrm\ICMRM.properties
```

On AIX:

```
/usr/WebSphere/AppServer/installedApps/icmrm.ear/icmrm.war
/WEB-INF/classes/com/ibm/mm/icmrm/ICMRM.properties
```

On Solaris:

```
/opt/WebSphere/AppServer/installedApps/icmrm.ear/icmrm.war
/WEB-INF/classes/com/ibm/mm/icmrm/ICMRM.properties
```

Update your ICMRM.properties file as shown in the following example with the following assumptions:

- You installed and deployed the resource manager with the default values on a Windows NT machine named ERIN
- The TSM API client is installed on c:\tsm
- You created a unique TSM API node id of **icmrm**
- You configured a TSM options file with the appropriate information and named it **c:\cm81\icmrm.opt**

With the assumptions listed, you would need to update the ICMRM.properties file with the information shown in Table 164.

Table 164. Properties file example

TSM API variable	Description	Value	ICMRM.properties value
DSMI_CONFIG	Points to TSM API options file	`c:\cm81\icmrm.opt`	`c\:\\cm81\\icmrm.opt`
DSMI_DIR	Points to TSM API message file dscameng	`c:\tsm\api`	`c\:\\tsm\\api`
DSMI_LOG	Points to TSM API log file	`c:\cm81\tsmapi.log`	`c\:\\cm81\\tsmapi.log`
(optional) TSMBufferSize	TSM buffer size	131072 (default)	131072 (default) maximum = 1M

If these TSM settings do not point to the correct location, you will have unpredictable results when using the system administration program to define TSM volumes, or when the resource manager attempts to access the TSM server. Do not enable the TSM device driver for the resource manager unless your system meets the following conditions:

- The TSM client is installed on the resource manager machine.
- A TSM server is installed and accessible through the TSM client APIs and has a defined Domain and Policy set.
- The resource manager runs on a workstation located in the same LAN domain as the TSM server.

The TSM server can reside on the same machine (or node) as the resource manager. This improves communications performance, but divides processor performance between both servers.

If you install the TSM server and resource manager on different machines, the resource manager will be able to interact with a TSM server on any TSM-supported platform. The TSM-supported platforms include:

- Windows
- AIX
- Solaris

Configure the resource manager using the Content Manager system administration client

To configure the resource manager using the system administration client, you need to perform the following steps:

1. Define a new server
2. Define a new storage class
3. Define a new Tivoli Storage Manager volume in the storage systems
4. Enable the Tivoli Storage Manager device manager

1. Define a new server

To define a new server:

1. Open the Content Manager system administration client
2. In the left navigation panel of the System Administration Client window, expand the tree to find the name of the resource manager.
3. Expand the tree under the resource manager, and click **Server Definitions**.
4. The **New Server Definition** window opens. Fill in the fields as follows:
   a. In the **Name** field, enter the name of your TSM server (example: NATHAN).
   b. In the **Server type** field, select ″Tivoli Storage Manager″ from the drop-down list.

c. In the **Hostname** field, enter the fully qualified hostname of your TSM server (example: NATHAN.xxx.us.com).

d. In the **User ID** field, enter the TSM User ID that you set up for you TSM server (example: icmrmwn2).

e. In the **Password** field, enter the password for your user ID.

f. In the **Protocol** field, select ″ftp″ from the drop-down list.

g. In the **Port number** field, enter a port number (any number will work for TSM)

h. You can leave the **Schema** field blank, or you can enter anything you want (anything will work)

i. You can leave the **Path** field blank (anything will work)

5. Click **OK**.

2. Define a new storage class

To define a new Storage Class:

1. Right-click **Storage Classes**, then click **New**.
2. The New Storage Class window opens.
   a. Enter TSM in the **Name** field.
   b. Select **Local destination**.
   c. Select ICMADDM from the drop-down list of the **Device manager** field.
3. Click **OK**.

3. Define a new Tivoli Storage Manager volume in the storage system

To define a new TSM storage manager volume in the storage system:

1. Expand the tree under **Storage Systems**.
2. Right-click **Tivoli Storage Manager**, then click **New**.
3. The New Tivoli Storage Manager Volume window opens.
   a. Enter DISK in the **TSM management class** field. DISK (case-sensitive) must be already defined in the TSM server.
   b. Select the server name from the drop-down list in the **Server name** field.
   c. Select TSM from the drop-down list in the **Storage class** field.
   d. Within the large **Assignment** box, select **Assigned**, then check the group number(s) that you want this volume to be assigned to.
4. Click **OK**

4. Enable the Tivoli Storage Manager device manager

To enable the Tivoli Storage Manager Device Manager (for Device Manager Properties - ICMADDM):

1. Right-click **Device Managers**, then click **ICMADDM**.

2. The Device Manager Properties - ICMADDM window opens.
   a. The **Name** field should have ICMADDM (greyed out) shown.
   b. Enter information into the **Description** field (for example: ADSM DEVICE MANAGER).
   c. The **Parameters** field can be left blank.
   d. Enter TSM in the **Class** field.
   e. Click to select **Enable** for the **Device manager**.
3. Click **OK**.

For more information, see ″Creating a migration policy″ in the ″Managing databases″ section of the *System Administration Guide*.

Each TSM volume defined for the resource manager results in a unique TSM file space on the TSM server. The name of the file space is:

```
/ICM/resource-manager-name/resource-manager-collection/TSM-management-class
```

When you store the first object into each unique Content Manager TSM volume, a TSM file space is created.

When you delete or migrate all of the objects out of the TSM file space, the initial file space is not deleted.

If you want to delete an empty file space, use the TSM administration functions to delete it.

Step 5. Customizing the resource manager to use specific TSM management classes

It is recommended that you specify a TSM management class like the example “TSM include file for resource manager RMAIX on AIX machine NATHAN (TSMmc.inc)” on page 437.

If the management class is left unspecified, the default TSM management class will manage all the objects stored in TSM by the resource manager. If it is not modified, the default TSM management class will expire stored objects in a year.

If you do not assign a specific management class to files, TSM uses the default management class in the active policy set of your policy domain.

To customize the resource manager if you do not have an active policy set of your policy domain, you must include the TSM/CM management class in your TSM client options file.

Step 6. Determining the space available in TSM

Content Manager does not check for a full TSM management class. The defined Content Manager volume pointing to TSM is considered to be infinite in size.

Step 7. Using overflow storage systems

If a storage class has both file systems (AIX) or volumes (Windows) and TSM storage systems assigned to a storage group, the file system or volume is used for storing objects first. When all the assigned file systems or volumes are full, objects are stored to TSM.

If a storage class has both a file system or volume and a TSM storage system marked as overflow storage systems, the first available overflow storage system, based upon its creation date, is used when all the assigned storage systems are full. For example, if `TSM_mc_1` (TSM) and `/vol2` (file system) are marked as overflow storage systems; `TSM_mc_1` is selected first by the system because it was created first. In this case, because `TSM_mc_1` is considered to be infinite, `/vol2` can never get assigned to this storage group unless the suspend storage flag for `TSM_mc_1` is turned on.

When the first object is stored to a storage system that is marked as overflow, the storage system is assigned to the storage group to which the object belonged.

TSM acts as an infinite object storage repository. The TSM system administrator is responsible for ensuring that all the storage pool volumes associated with the target management class are online and have sufficient storage space for backing up objects. As a result, the concept of using a TSM management class as an overflow storage system is different than using a volume or file system as an overflow storage system. The following examples illustrate the differences.

Example: AIX file system

Two file systems have been defined as storage systems, and they are associated with the same storage class. The storage class is associated with the fixed disk device manager. The two file systems are defined as follows:

/vol1 Assigned to a storage group

/vol2 Marked as overflow volume

If one of the following conditions occurs while the resource manager is running, objects will be stored to the overflow file system, /vol2 (assuming that it is mounted):

- /vol1 is unmounted, and the directory over which it is mounted is removed.

- /vol1 is mounted, but it is full.
- /vol1 is mounted and is not full. However, the suspend storage flag for /vol1 is turned on.

Example: Windows volume

Two volumes have been defined as storage systems, and they are associated with the same storage class. The storage class is associated with only a fixed disk device manager. The two volumes are defined as follows:

VOLUME1
Assigned to a storage group

VOLUME2
Marked as an overflow volume

If one of the following conditions occurs when the resource manager is running, objects are stored to the overflow volume, VOLUME2, (assuming that it is online):

- VOLUME1 is offline.
- VOLUME1 is online, but it is full.
- VOLUME1 is online and is not full. However, the suspend storage flag for VOLUME1 is turned on.

Example: AIX or Windows TSM

Two TSM management classes have been defined as storage systems, and they are associated with the same storage class. The storage class is associated with the TSM device manager. The two volumes are defined as follows:

TSM_mc1
Assigned to a storage group

TSM_mc2
Marked as an overflow volume

Objects are stored on the overflow volume only if the suspend storage flag for TSM_mc1 is turned on.

Objects are not stored to the overflow TSM management class in any of the following conditions:

- All the storage pool volumes associated with TSM_mc1 are full.

  The TSM system administrator needs to ensure that there is enough storage space that is assigned for the TSM management class.
- All the storage pool volumes associated with TSM_mc1 are offline.

  The TSM system administrator needs to ensure that all volumes associated with the TSM management class are online.

Troubleshooting TSM and the Content Manager resource manager

If a resource manager fails to start, check the error log for any reported errors. The problem might be caused by one of the conditions shown in Table 165:

Table 165. Resource manager error conditions

Error	Possible solution
The environment variables are not set properly.	Check to be sure that the environment variables are set correctly for your system. The environment variables are: DSMI_CONFIG DSMI_DIR DSMI_LOG
The TSM server is not active.	Make sure the TSM server is active and enabled.
The resource manager cannot establish a communication link to the TSM server.	Make sure the resource manager node on the TSM server is unlocked.
The file systems assigned to the resource manager are not online.	Make sure all the assigned file systems are mounted. For the storage systems for TSM, make sure the policy set to which they are associated is active. The resource manager cannot store or retrieve objects to or from a TSM management class whose associated policy set is not active.

If an active resource manager reports a problem accessing TSM, verify that TSM is active. If TSM is not active, restart it.

Recommendation: For AIX, before you start an resource manager, make sure that all the file systems defined as storage systems are mounted. If a file system is not mounted, and the directory over which it was mounted still exists, objects will be stored to that directory. Objects might be lost when the corresponding file system is mounted over that directory.

Chapter 31. Configuring Enterprise Information Portal components

This section explains how to configure the EIP components.

Configuring the components on Windows

This section explains how to connect the administration client to a local and a remote administration database, and how to start the services and utilities required to support workflow.

Important: You must know the local and/or remote database connect-only or administrator user ID and password of the database you are connecting to. The default administrator information is `ICMADMIN/password`. The administrator and connect-only user IDs must be created on the local administration client workstation before you can log on to either a local or remote database.

Connecting the administration client to a local administration database

If you install an administration database on the same server where you install the administration client, the information required to connect the local client and server is already stored in `cmbds.ini`, a file that stores database connection information. You do not have to perform any post-install configuration and can connect immediately using the steps in this section. **Requirement:** If you create additional local databases using the EIP Database Install utility, you must manually modify the `cmbds.ini` with the required information before you can connect to the new database.

1. Click **Start-->Programs-->Enterprise Information Portal for Multiplatforms 8.2-->Administration**
2. Select the local database from the drop-down list in the Server field.
3. Type the administrator user ID and password and press OK.
4. The system administration client opens. **Tip:** If you used EIP First Steps, the sample databases are displayed in the left pane of the client.

Connecting the administration client to a remote administration database

There are two ways to connect an EIP administration client to a remote AIX, Windows or Solaris database:

- Connect through an RMI server (see Chapter 33, “Configuring an RMI server”, on page 507).
- Define a connection by cataloging the database using DB2 Configuration Assistant, and then defining server connection parameters using the EIP

Server Configuration Utility. The utility copies information, such as the database schema name, alias name, operating system and so forth, to a file named `cmbds.ini`. When you launch the system administration client, the list of servers that you can log into is taken from the servers defined in `cmbds.ini`.

Requirement: You must catalog each remote database separately. Every remote database must be listed in the `cmbds.ini` file before you can connect to it from the administration client.

Tip: If you are an experienced user, you can skip the Server Configuration Utility steps and modify the `cmbds.ini` in a text editor. The default path to `cmbds.ini` is `C:\Program Files\IBM\CMgmt`.

Important: If the person who installed the product already configured the database catalog values for the remote database you want to connect to, you do not have to perform the DB2 CCA steps for that database. But if the installer did not type the database catalog values or you want to connect to an additional remote database, you must use DB2CCA and modify the `cmbds.ini` file with the connection parameters for the additional database(s).

Step 1 - catalog remote database using DB2 Configuration Assistant

The DB2 Configuration Assistant (CCA) catalogs the remote EIP database in DB2. Tocatalog the remote database using DB2CCA, you must know the remote server hostname, the database name and database instance port number, and you must define an alias for the remote database.

Steps 1a - 1f explain how to locate the database name, schema name and connection port number. You must know the names and the connection port number to configurhe names and port numbers ato configure a connection between the administration client and a remote database.

1. Locate the remote database connection information:
   a. Log in to the remote AIX, Windows or Solaris server with a user ID that has DB2 administratin authority.
   b. Type `db2 list db directory`
   c. Select the name of the administration database you want to connect to. Note of the db2 instance that the database is installed on, because different instances can have different connection port numbers.
   d. Type `db2 connect to <database> user <userID> using <password>`
   e. Type `db2 list tables` and make a note of the database schema name (required by the server configuration utility).
   f. Locate the connection port number associated with the remote administration database:

      On Windows:

1) Open the DB2 Control Center on the remote Windows server.

2) Right click one of the available instances for the local machine.

3) Select ″Setup Communications...″.

4) Select the ″Properties″ button to the right of the TCP/IP choice. The port number will be listed on the window.

On AIX or Solaris

1) Type `cd /usr/etc`

2) Type `cat services`

3) Scroll through the list of services until you find the connection port number for the database instance of the remote database. For example, if the database is installed on `db2inst1`, the connection port might be `50000`.

4)

2. Use the DB2 Configuration Assistant to catalog the remote database. Consult the DB2CCA help files for more information.
   a. Log in to the Windows server where the administration client is installed. You must log in with a user ID that has full DB2ADM privileges.
   b. Navigate to the DB2 Configuration Assistant from the Start-->Programs menu..
   c. Follow the DB2 Configuration Assistant prompts to catalog and test the connection to the remote database.
   d. If the DB2 CCA connection test was successful, follow the steps in “Step 2 - use the Server Configuration Utility”, or modify the cmbds.ini file directly to define the remote database connection parameters t stored in `cmbds.ini`

Step 2 - use the Server Configuration Utility

The server configuration utility prompts you for connectivity information (port number, hostname, etc.) about the remote database and stores the data in `cmbds.ini`.

1. Click **Start-->Programs-->IBM Enterprise Information Portal for Multiplatforms-->Server Configuration Utility**.

2. Type the information in the fields (see Table 166).

Table 166. Server configuration utility

Field	Information	Notes
Server	Select database type, either Content Manager or EIP.	Server means the database type, not the name of the server where the database is installed. **Tip:** You can use the administration client to manage both database types only if your system includes Content Manager and EIP administration clients on the same machine.
Server name	Type the alias name of the database you are connecting to. Requirement: You must use the same alias name defined in DB2CCA.	An alias provides a unique name that identifies the remote database on your workstation. Alias names have an eight-character limit. For example, if the remote database name is ICMNLSDB, an alias could be REMOTE1.
Schema name	Type the schema name assigned when the remote database was created.	ICMADMIN is the default schema name for the EIP and Content Manager databases.
Host name	Type the name of the computer where the remote database was installed.	Type the fully-qualified hostname or type an IP address of the computer where the remote database is installed.
Operating system	Select an operating system from the drop-down box.	Select AIX, Sun Solaris or Windows. The OS/390 option is not functional in EIP 8.2.
Port number	Type the port number assigned to the remote database.	50000 is the default connection port number for EIP and Content Manager databases installed on Windows, AIX and Solaris.
Remote database name	Type the name of the remote database. Use capital letters.	ICMNLSDB is the default name for the EIP and Content Manager databases.

Table 166. Server configuration utility (continued)

Field	Information	Notes
Node name	Type the node name of the remote EIP or Content Manager database.	The node name is a unique name assigned to the remote database, similar to the alias name you create for the remote database. To find the node name of a database installed on a Windows, AIX or Solaris server: a. Open a db2 command line session. b. At the `db2=>` prompt, type `LIST NODE DIRECTORY` c. DB2 displays node names and other data for all databases installed or defined on the remote server.
Enable single sign-on	Click if single sign-on was enabled during database installation.	The default setting is unchecked (disabled).
Security options	Click client authentication if that option was selected during database creation.	The default setting is Server.

3. Click OK.
4. Test the connection to the remote database.
   a. Click **Start-->Programs-->Enterprise Information Portal for Multiplatforms 8.2-->Administration**.
   b. Select the remote database name from the drop-down list in the Server field. The name matches the alias you defined in the Server Configuration Utility.
   c. Type the remote database administrator or connect-only user ID and password and click OK.

Step 3 - test the remote database connection

1. Log in to the Windows server where the administration client is installed.
2. Click **Start-->Programs-->Enterprise Information Portal for Multiplatforms 8.2-->Administration**.
3. Select the remote database alias name from the drop-down list in the Server field. The name matches the alias you defined in the Server Configuration Utility and in DB2 Configuration Assistant.
4. Type the user ID and password associated with the remote database.

5. Cick OK. The administration client opens.

Configuring workflow services and utilities on Windows

Before you can use workflow, you must start workflow services and utilities. The steps you take depend on how you installed MQSeries products.

Restriction: Because the administration database contains the functionality required to use workflow, the administration database must be installed on a server that has DB2 Universal Database, MQSeries Server and MQWorkflow. The administration client, where you administer workflow, can be local or remote.

Configuring MQSeries if you used EIP custom installation

See “Configuring MQSeries Workflow on Windows” on page 97.

Configuring MQSeries Workflow if you did not use EIP custom installation

1. Start the MQSeries server as an NT service.
2. Create default users by importing `CMBWFAdmin.fdl` into the MQSeries Workflow database.
3. Run the following utility from a command prompt:

   ```
   fmcibie -i CMBWFAdmin.fdl -uadmin -ppassword -o
   ```
4. At a windows command prompt enter the following command on one line:

   ```
   @ECHO DEFINE QLOCAL (EIPWFEVENT) DESCR('Local EIP WF queue for events')
    | runmqsc FMCQM
   ```

Setting the environment variables for the development toolkit

If you installed the connector toolkit and samples, you must set the environment before you can use the samples.

On Windows, click **Start**→Programs →IBM Enterprise Information for Multiplatforms 8.2 Development Window→

You only have to set the environment variables once.

Using a sample program from the connector toolkit

The example below describes how to use the sample java program on Windows servers to test the connection to an OnDemand server:

1. Set the development environment by click Start-->Programs-->Enterprise Information Portal for Multiplatforms 8.2-->Development Window. A command prompt appears that displays `C:\CMBROOT`.
2. Change to SAMPLES\java\od

3. Compile the sample connection test program by typing `javac TConnectOD.java`
4. Test the sample program by typing `java TConnectOD <libSrv> <userID> <pw> <connect string>`
5. If the connection test is successful, the program displays connection and disconnection status information. If the test is not successful, the program displays an exception message.

You can view all the sample programs in a text editor. The sample programs will list the variables required to operate the program. Each directory that contains samples also includes documentation. The documentation explains the system parameters required to work with the sample programs, and also lists the sample program names and the tasks each program can carry out.

Defining a content server

This section describes how to log in to the administration client and define a content server.

1. Click **Start ⟶Programs⟶IBM Enterprise Information for Multiplatforms 8.2⟶Administration**.
2. Select a database.
3. Type the database administrator ID and password you used to catalog or add the database.
4. Click **OK**.
5. The administration client window appears and the database name is displayed in the left pane.

To define and test a connection to a DB2 content server, and create an icon for it, complete the following steps:

1. From the `<database name>` tree, right-click **Server** and click **New**. The New Server Connection window opens.
2. From the list of content servers, select **DB2**. The New Server: DB2 window opens.
3. Click the **Initialization Parameters** tab.
4. In the **Connect string** field, type `SCHEMA=<schema name defined when server was installed>`.
5. Click **Test Connection**.
6. If EIP cannot log in to the database using the user ID and password you entered when logging in to the client, EIP prompts you for the user ID and password for the administration database.
   a. In the **User ID** field, type `<user ID defined when database was installed>`.

   b. In the **Password** field, type `<password defined when database was installed>`.
   c. Click **OK** to log on and close the window.

   The following message displays: `The connection to <database name> was successful.` Click **OK**.
7. Click **OK** to close the New Server: DB2 window and create the `<server name>` icon.

Congratulations! You have successfully installed the Enterprise Information Portal server with the DB2 connector.

To access the sample metadata from Enterprise Information Portal, complete the following steps:

1. From the Enterprise Information Portal administration client main window, right-click the <server name> icon and click **Refresh Server Inventory**.
2. If you are not already logged on to the Sample database, the Logon Sample window opens. Log on to the `<database name>` database:
   a. In the **User ID** field, <user ID defined when database was installed>.
   b. In the **Password** field, type <password defined when database was installed>.
   c. Click **OK** to log on and close the window.

   The following message displays: `The server inventory has been refreshed.` Click **OK** to continue.
3. Click **Tools** ⟶ **Server Inventory Viewer**. The Server Inventory Viewer opens, displaying the sample data.
4. Close the Server Inventory Viewer.
5. Close the administration client main window.

Configuring workflow on AIX and Solaris

Before you can use workflow, you must start workflow services and utilities. The steps you take depend on how you installed MQSeries products.

Restriction: Because the administration database contains the functionality required to use workflow. the administration database must be installed on a server that has DB2 Universal Database, MQSeries Server and MQSeries Workflow.

Configuring MQSeries if you used EIP custom installation

1. Verify that MQSeries is running as an NT service.
2. Change to the directory where you installed workflow.
3. Using a command prompt, run `./cmbwfstart.sh`

4. Start the user exit utility. In a command window, run `fmcxspea -u=ADMIN -p=password`. The user exit utility provides workflow batch processing.

Configuring MQSeries if you did not use EIP custom installation

1. Start the MQSeries server.
2. Create default users by importing `CMBWFAdmin.fdl` into the MQSeries Workflow database. Run the following utility from a command prompt: `fmcibie -u ADMIN -p password -i CMBWFAdmin.fdl`
3. Remove (or comment out) the statement:

   ```
   set PATH=C:\progra~1\MQSeri~1\bin\MQServer;%PATH%
   ```

   in the following files:

   - `cmbenv81.bat`
   - `cmbfestart81.bat`
   - `cmbsvregist81.bat`
4. Start the `upes` utility:

   ```
   ./cmbupes81.sh
   ```
5. Start the user exit utility. In a command window, run `fmcxspea -u=ADMIN -p=password`.

Configuring the Web Application Server for the EIP tag library and servlet

This section explains how to configure the tag library and servlets installed with the connector toolkit. The servlets and tags help you write EIP applications.

Before you can configure the servlets and tags, you must install and configure IBM WebSphere Application Server Version 5.0. See the WebSphere documentation for hardware and software requirements.

Building the WebSphere Application Resource (WAR) file

The following must be installed and operating on the server before configuring the tag library and servlet: IBM WebSphere Application Server Version 5.0 (see the WebSphere documentation for hardware and software requirements)

Creating the web module

1. Start the WebSphere Administrator’s Console.
2. From the console menu, select **Tools⟶Application Assembly Tool** (AAT). You see a window displaying different wizards. Click **Cancel**.
3. Create a new web module by selecting **File⟶New⟶Web Module**.
4. Specify `eip` for the display name. Click **Apply**.

5. Select **File**→**Save As** and save the file as `cmbroot\samples\modules\eip.war`

Adding the jar files

1. Expand the Files category. You will see Class Files, Jar Files and Resource Files.
2. Right-click Jar Files and select **Add Files**. You will see the Add Files window.
3. Click **Browse**. Select `cmbroot` as the root directory.
4. Click subdirectory `LIB` so that `LIB` appears in the **File** name box.
5. Click **Select**. From the upper right box in the Add Files window, select the files listed below. **Tip:** T select more than one file, hold down the **Ctrl** key and click the file.

```
cmb81.jar
cmbcm81.jar
cmbsdk81.jar
cmbservlets81.jar
cmbtag81.jar
cmbview81.jar
esclisrv.jar
essrv.jar
log4j.jar
cmblog4j.jar
```

6. Click **Add**. The files appear in the Selected Files box.
7. Click **OK**. You should see the jar files in the upper right window of the AAT.

Adding the JSP files

1. Right-click Resource Files. Select Add Files. You see the Add Files window.
2. Click **Browse**.
3. Select `cmbroot` as the root directory.
4. Click the subdirectory `samples` so that `samples` appears in the File name box below.
5. Click **Select**. In the upper right window, select `jsp`.
6. Click **Add**. The files appear in the Selected Files box.
7. Click **OK**. You should see the JSP and HTML files in the upper right window of the AAT.

Adding the tag library

1. Right-click **Resource Files**, and select **Add Files**. You will see the Add Files window.
2. Click **Browse** and select `cmbroot` as the root directory.
3. Click the subdirectory `LIB` so that `LIB` appears in the File Name box below.

4. Click **Select**. In the upper right window, select `tld`.
5. Click **Add**. The file `taglib.tld` will appear in the Selected Files box.
6. Click **OK**. You should see the `taglib.tld` along with the JSP files in the upper right window of the AAT.

Defining an alias for the tag library

1. In the left window of the AAT, right-click **Tag Libraries** and select **New**.
2. Specify `cmb` for the Tag Library file name. Specify `taglib.tld` for the tag library location. Click **OK**.

Defining the controller servlet

1. In the left window of the AAT, right-click Web Components and select **New**.
2. Specify `control` as the Component name. Specify `control servlet` as the Display name. Under Component Type, make sure that the **Servlet** radio button is selected.
3. Click **Browse** button to the right of the Class name field. In the left window, expand `WEB-INF`, expand `lib`, expand `cmbservlets81.jar` to `com`→`ibm`→`mm`→`servlets`.
4. Click the servlets subdirectory. In the right window, select `CMBControlServlet.class`.
5. Click **OK**. You should see `com.ibm.mm.servlets.CMBControlServlet` in the Class name field.

   Now define the initialization parameter that specifies the location of the properties file. You should see control servlet under Web Components in the left window.
6. Expand control servlet. Right-click Initialization Parameters, and select **New**.
7. Specify `servletPropertiesURL` as the Parameter name.
8. Specify `/com/ibm/mm/servlets/cmbservlet.properties` as the parameter value.
9. Click **OK**.

Defining the servlet mapping for the controller servlet

1. In the left window of the AAT, right-click Servlet Mapping. Select **New**.
2. Specify `/jsp/servlets/CMBControlServlet` as the URL pattern.
3. Select `control` as the Servlet.
4. Click **OK**.
5. Select **File**→**Save** to save the `WAR` file.

Building the Enterprise Application Resource file

In this section, you configure the components used to build the Enterprise Application Resource (EAR) file.

Building the EAR file

1. Close the WAR file by selecting **File→Close**.
2. Select **File→New→Application**.
3. Specify `eip.ear` as the Display name, and click **Apply**.
4. Add the WAR file. Right-click the Web Modules category and select **Import**.
5. Select `cmbroot\samples\modules\eip.war`. Specify `/eip` as the Context root. Click **OK**.
6. Select **File→Save As**, and specify `cmbroot\modules\eip.ear` as the name.

Installing the application

1. Close the AAT.
2. Start the WebSphere Administration Console.
3. Select **Console→Wizards→Install Enterprise Application**. Make sure your node is selected in the **Browse for file on node** field.
4. Select `Install Application (*.ear)`.
5. Click the **Browse** button to the right of the Path field.
6. Select `cmbroot\samples\modules\eip.ear`. Click **Open**. You should see `C:\cmbroot\SAMPLES\modules\eip.ear` in the Path field. Specify `eip.ear` as the Application name.
7. Click **Next** several times until you see the Selecting Application Servers page. You can select the Default Server or another if you have another defined.
8. Click **Next**, then click **Finish**.

Running the servlet

This section explains how to run the servlet. **Requirement:** When WAS 5 security is enabled, create a `was.policy` file in the `eip.ear\META-INF` subdirectory before running the servlet.

1. Stop and restart your application server under Nodes->*your node*->Application Servers->*your server.*
2. Open your browser and point to http://localhost:9080/eip/jsp/main.html, and follow the links to either the tag library samples or the servlet actions. You may also access either directly by pointing to http://localhost:9080/eip/jsp/servlets/actions.html for the list of available servlet actions or by pointing to"http://localhost:9080/eip/jsp/taglib/index.html for the list of available tags.

Using the Panagon Image Services (IDMIS) 3.5.0 content server

You need to install the Panagon Image Services (IDMIS) 3.5.0 and the Panagon Image Services Toolkit 3.5.0. See Content Connector For Panagon Image Services Install Guide. You also need to install two fixes:

- SCR 133231 - Fix for wal_sysv.dll and wal_ipc.exe
- SCR 133232 - Fix for wal_sec.dll

These fixes are available from the FileNET Corporation. If you have the proper licenses, you should be authorized to ftp the fixes from the FileNET website, or else you can contact your FileNET sales representative.

You also need to do the following:

1. Add the following jar files to the eip.ear file. Follow the same procedure as in "Building the WebSphere Application Resource (WAR) file" on page 455.
   - `cmbfn81.jar`
   - `cmbfnc81.jar`
2. Go to the WebSphere Administration Console. Select your server under Application Servers. On the right side, under the General tab, press the Environment button. You should see the Environment Editor. Press Add. Under Name, add ″PATH″. Under Value, add `c:\fnsw\client\bin;c:\fnsw\client\shobj`. Press Apply. Stop and restart the server.

   Tip: This step is not necessary if the information is already in the Path system environment variable.

Using the Domino.Doc content server

You must install the Domino.Doc desktop client.

After applying service

If you apply an EIP service update, you must refresh the jar files in eip.war. Copy the following jar files from `cmbroot\lib` into `websphere\appserver\installedapps\eip.ear\eip.war\WEB-INF\lib:`

- cmb81.jar
- cmbcm81.jar
- cmbsdk81.jar
- cmbservlets81.jar
- cmbtag81.jar
- cmbview81.jar
- esclisrv.jar
- essrv.jar
- cmblog4j.jar

Then stop and restart the application server.

Installing and configuring Information Mining

This section describes how to install and configure the Information Structuring Tool and the JSP sample using WAS.

Installation scenarios

The Information Structuring Tool and the Information Mining Java Server Page application (JSPs, for details refer to) can be deployed on a single workstation, or on two different workstations. In the following sections, the installation descriptions are written for the Information Structuring Tool. For the JSPs, replace Information Structuring Tool by JSPs.

- For Windows:
  - `<CMBROOT>` is the value of the corresponding environment variable, for example, `d:\cmbroot`
  - `<DB2HOME>` is the value of the corresponding environment variable, for example, `d:\sqllib`
  - `<CMCOMMON>` is the value of the corresponding environment variable, for example, `c:\Program Files\IBM\CMGMT`
- For AIX:
  - `<DB2HOME>` is the directory where DB2 is installed, for example, `/usr/lpp/db2_07_01` or `/usr/opt/db2_08_01`

    `<DB2JAVAHOME>` is the directory where the Java 1.2 library files are located. For DB2 V7, this is `<DB2HOME>/java12` and for DB2 V8, `<DB2HOME>/java`
- For Solaris:
  - `<DB2HOME>` is the directory where DB2 is installed, for example, `/opt/IBMdb2/V7.1` or `/opt/IBM/db2/V8.1`

    `<DB2JAVAHOME>` is the directory where the Java 1.2 library files are located. For DB2 V7, this is `<DB2HOME>/java12` and for DB2 V8, `<DB2HOME>/java`

Single workstation

1. Install the Enterprise Information Portal server with the information mining feature.
2. Install the WAS.
3. Deploy the Information Structuring Tool.

Client-server setup

If the Information Structuring Tool and the information mining feature are deployed on different workstations, carry out the following:

On workstation A:

- Install the Enterprise Information Portal server with the information mining feature.
- Start the RMI server.
- For Windows:
  - Open file `c:\Program Files\IBM\CMGMT\cmbsvregist81.bat`
  - Locate the line starting with `set CLASSPATH=`
  - Check that the CLASSPATH contains the following entries: `<DB2HOME>\java\db2java.zip;<JARDIR>\cmbcm81.jar;`
  - Save `cmbsvregist81.bat`
- For AIX:
  - Open file `/usr/lpp/cmb/cmgmt/cmbsvregist81.sh`
  - Locate the line starting with `export CLASSPATH=`
  - Check that the CLASSPATH contains the following entries: `<DB2HOME>/java/db2java.zip:$JARDIR/cmbcm81.jar:`
  - Save `cmbsvregist81.sh`
- For Solaris:
  - Open file `/opt/IBMcmb/cmgmt/cmbsvregist81.sh`
  - Locate the line starting with `export CLASSPATH=`
  - Check that the CLASSPATH contains the following entries: `<DB2HOME>/java/db2java.zip:$JARDIR/cmbcm81.jar:`
  - Save `cmbsvregist81.sh`

On workstation B:

- Install the WAS.
- Install the Enterprise Information Portal client.
- Locate the files `cmbsvclient.ini` and `cmbsvcs.ini` at:
  - For Windows: `<CMCOMMON>`
  - For AIX: `/usr/lpp/cmb/cmgmt`
  - For Solaris: `/opt/IBMcmb/cmgmt`
- In file `cmbsvclient.ini`, `RemoteHost` must be set to the name of **workstation A**.
- In file `cmbsvcs.ini`, `IKF` must be **remote**.
- Copy all three files to the working directory of the application server where the Information Structuring Tool will be deployed:
  - For WAS AEs:
    - For Windows: `<WAS_HOME>\bin`
    - For AIX: `/usr/WebSphere/AppServer/bin`
    - For Solaris: `/opt/WebSphere/AppServer/bin`

- For WAS AE:
  - Open an administrative console.
  - Select the application server in the tree view.
  - Select the **General** tab. The directory can be found under ″Working Directory″.
- Deploy the Information Structuring Tool.

Configuring the Web Application Server for the Information Structuring Tool

Before you can install the Information Structuring Tool on the Websphere Application Server Advanced Edition (WAS 4 AE) or Advanced Edition Single Server (WAS 4 AEs), or Websphere Application Server 5 Base or Websphere Application Server 5 Network Deployment (ND), you need the following information:

- `<Node>` is the name of the workstation where the Information Structuring Tool is to be installed
- `<AppServer>` is the Application Server on `<Node>` where the Information Structuring Tool is to be installed, for example, for WAS 4 `Default Server` or for WAS 5, `server1`
- `<VirtualHost>` is the name of the virtual host the Information Structuring Tool is to run on, for example, `default_host`
- `<WebPath>` is the path portion of the URL used to access the Information Structuring Tool. This path **must** end with `/IST`. For example, if the Information Structuring Tool is installed on the server `prefix` and `<WebPath>` is `/webApps/IST`, a possible URL to access the Information Structuring Tool could be `http://prefix/webApps/IST/login.html`
- `<WAS_HOME>` is the directory where the WAS is installed on `<Node>`, for example, `d:\WebSphere\AppServer` on Windows, `/usr/WebSphere/AppServer` on AIX and `/opt/WebSphere/AppServer` on Solaris.
- WAS 5 only: `<Cell>` is the name of the administrative cell. For WAS 5 Base, this is the same as `<Node>`. For WAS 5 ND, this is the name of the workstation the deployment manager is running on.

WAS V4

The following section describes the IST deployment procedure in WAS AEs, followed by WAS AE.

WAS AEs: After installing the WAS AEs and Enterprise Information Portal, open the WAS Administrator’s Console and carry out the following:

1. From the console menu, select **Nodes⟶<Node>⟶Application Server⟶<AppServer>⟶Process Definitions⟶JVM Settings**
2. If the WAS and Enterprise Information Portal are on the same workstation, enter the following `Classpath` information:

- For Windows:

  ```
  <CMBROOT>\ikf\lib
  <CMBROOT>\ikf\lib\ikf.jar
  <CMBROOT>\lib\cmb81.jar
  <CMBROOT>\lib\cmbsdk81.jar
  <CMCOMMON>
  <CMBROOT>\lib\cmblog4j81.jar
  <CMBROOT>\lib\log4j.jar
  <DB2HOME>\java\db2java.zip
  ```

- For AIX:

  ```
  /usr/lpp/cmb/ikf/lib
  /usr/lpp/cmb/ikf/lib/ikf.jar
  /usr/lpp/cmb/lib
  /usr/lpp/cmb/lib/cmb81.jar
  /usr/lpp/cmb/lib/cmbsdk81.jar
  /usr/lpp/cmb/cmgmt
  /usr/lpp/cmb/lib/cmblog4j81.jar
  /usr/lpp/cmb/lib/log4j.jar
  <DB2JAVAHOME>/db2java.zip
  ```

- For Solaris:

  ```
  /opt/IBMcmb/ikf/lib
  /opt/IBMcmb/ikf/lib/ikf.jar
  /opt/IBMcmb/lib
  /opt/IBMcmb/lib/cmb81.jar
  /opt/IBMcmb/lib/cmbsdk81.jar
  /opt/IBMcmb/cmgmt
  /opt/IBMcmb/lib/cmblog4j81.jar
  /opt/IBMcmb/lib/log4j.jar
  <DB2JAVAHOME>/db2java.zip
  ```

  If the WAS and Enterprise Information Portal are on different workstations, the `Classpath` information is as follows:

  - For Windows:

    ```
    <CMBROOT>\ikf\lib\ikf.jar
    <CMCOMMON>
    <CMBROOT>\lib\cmb81.jar
    ```

  - For AIX:

    ```
    /usr/lpp/cmb/ikf/lib/ikf.jar
    /usr/lpp/cmb/lib/cmb81.jar
    /usr/lpp/cmb/cmgmt
    ```

  - For Solaris:

    ```
    /opt/IBMcmb/ikf/lib/ikf.jar
    /opt/IBMcmb/lib/cmb81.jar
    /opt/IBMcmb/cmgmt
    ```

3. Set ″Maximum Heap Size″ to 512.
4. Click **OK** at the bottom of the page.
5. Save your configuration settings by clicking **Save** on the top bar of the WAS administrative console.

6. If the WAS and Enterprise Information Portal are on the same workstation:
   - For Windows:

     The PATH must be set in the WAS Administrative Console:
     - From the console menu, select **Nodes→<Node>→Application Server→<AppServer>→Process Definitions**
     - Under ″Advanced Settings″, select ″Environment″
     - In ″System Properties″, select ″New″
     - For ″property name″, enter PATH and for ″property value″, enter `<cmbroot>\ikf\bin`, for example, `d:\cmbroot\ikf\bin`
     - Select **OK**
     - Select **Save** on the top bar of the WAS administrative console
   - For AIX:

     The user who starts the Application Server, for example ″root″, must have the following line in the `.profile`, namely,

     ```
     . /usr/lpp/cmb/ikf/IST/bin/ISTSingleWorkstationEnv.sh
     ```
   - For Solaris:

     The user who starts the Application Server, for example ″root″, must have the following line in the `.profile`, namely,

     ```
     . /opt/IBMcmb/ikf/IST/bin/ISTSingleWorkstationEnv
     ```
7. Click **Exit** on the top bar of the console to exit.
8. Shut down the WAS by:
   - Switching to the directory `<WAS_Home>\bin` in a command shell
   - Entering:
     - For Windows: `stopserver`
     - For AIX: `./stopServer.sh`
     - For Solaris: `./stopServer.sh`
9. In the command shell, enter:
   - For Windows: `seappinstall -install <CMBROOT>\ikf\IST\IST.war`
   - For AIX: `./SEAppInstall.sh -install /usr/lpp/cmb/ikf/IST/IST.war`
   - For Solaris: `./SEAppInstall.sh -install /opt/IBMcmb/ikf/IST/IST.war`

   You are prompted as follows:
   - Please specify an application display name: Enter `IST`
   - Please specify a context root: Enter your `<WebPath>`, for example,`/webApps/IST` Ensure that `<WebPath>` ends in `/IST`
   - Do you wish to precompile all JSPs in this application: Enter `n`
   - Do you wish to precompile individual Web Applications: Enter `n`

- Please specify a virtual host for the following Web applications, IBM Information Structuring Tool: Enter your `<VirtualHost>`, for example, `default_host`

10. IST uses an EIP database named `icmnlsdb`

    If your database name is different:

    - Switch to the directory where the IST is deployed, typically at `<WAS_HOME>\installedApps`
    - Switch to the directory `IST.ear/IST.war/WEB-INF` and open the file `web.xml`
    - Search for `icmnlsdb` and rename to your EIP database.
    - Save the file.
11. Restart the WAS in the command shell by entering:
    - For Windows: `startserver`
    - For AIX: `./startServer.sh`
    - For Solaris: `./startServer.sh`
12. Re-generate the Web server plug-in configuration of WAS by:
    - Opening the Administrative Console
    - Selecting **Nodes—►<Node>—►Application Server—►<AppServer>**
    - Under ″Advanced Settings″, selecting ″Web Server Plugin Configuration″
    - Selecting ″Generate″
13. The URL to access the Information Structuring Tool is `http://host_alias/WebPath/login.html` where:
    - `host_alias` is one of the aliases specified for `VirtualHost`. To find this value:
      - Open the WAS Administrator's Console
      - From the console menu, select **Virtual Hosts—►<VirtualHost>—►Aliases**
      - Each entry in the list (Host Name and Port) is a valid host alias, for example, `prefix:9080`
    - `<WebPath>` you specified during installation, for example, `/webApps/IST`

WAS AE: After installing the WAS AE and Enterprise Information Portal, open the WAS Administrator's Console and carry out the following:

1. From the console menu, select **Nodes—►<Node>—►Application Server—►<AppServer>**
2. Stop the Application Server, if it is running.
3. Select the tab **JVM Settings** on the right.
4. If the WAS and Enterprise Information Portal are on the same workstation, enter the following `Classpath` information:

- For Windows:

  ```
  <CMBROOT>\ikf\lib
  <CMBROOT>\ikf\lib\ikf.jar
  <CMBROOT>\lib\cmbsdk81.jar
  <CMBROOT>\lib\cmb81.jar
  <CMCOMMON>
  <CMBROOT>\lib\cmblog4j81.jar
  <CMBROOT>\lib\log4j.jar
  <DB2HOME>\java\db2java.zip
  ```
- For AIX:

  ```
  /usr/lpp/cmb/ikf/lib
  /usr/lpp/cmb/ikf/lib/ikf.jar
  /usr/lpp/cmb/lib
  /usr/lpp/cmb/lib/cmb81.jar
  /usr/lpp/cmb/lib/cmbsdk81.jar
  /usr/lpp/cmb/cmgmt
  /usr/lpp/cmb/lib/cmblog4j81.jar
  /usr/lpp/cmb/lib/log4j.jar
  <DB2JAVAHOME>/db2java.zip
  ```
- For Solaris:

  ```
  /opt/IBMcmb/ikf/lib
  /opt/IBMcmb/ikf/lib/ikf.jar
  /opt/IBMcmb/lib
  /opt/IBMcmb/lib/cmb81.jar
  /opt/IBMcmb/lib/cmbsdk81.jar
  /opt/IBMcmb/cmgmt
  /opt/IBMcmb/lib/cmblog4j81.jar
  /opt/IBMcmb/lib/log4j.jar
  <DB2JAVAHOME>/db2java.zip
  ```

If the WAS and Enterprise Information Portal are on different workstations, the `Classpath` information is as follows:

- For Windows:

  ```
  <CMBROOT>\ikf\lib\ikf.jar
  <CMCOMMON>
  <CMBROOT>\lib\cmb81.jar
  ```
- For AIX:

  ```
  /usr/lpp/cmb/ikf/lib/ikf.jar
  /usr/lpp/cmb/lib/cmb81.jar
  /usr/lpp/cmb/cmgmt
  ```
- For Solaris:

  ```
  /opt/IBMcmb/ikf/lib/ikf.jar
  /opt/IBMcmb/lib/cmb81.jar
  /opt/IBMcmb/cmgmt
  ```

5. Set ″Maximum Heap Size″ to 512.
6. Select **Apply** at the bottom of the page.
7. If the WAS and Enterprise Information Portal are on the same workstation:

- For Windows:

  The server the IST is deployed in must contain an additional PATH entry:

  – From the console menu, select **Nodes→<Node>→Application Server→<AppServer>**
  – In the ″General″ tab, select ″Environment...″
  – In the Environment Editor frame, select ″Add″
  – For ″Name″, enter PATH and for ″Value″, enter `<cmbroot>\ikf\bin`, for example, `d:\cmbroot\ikf\bin`
  – Select **OK**
  – Select **Apply**
- For AIX:

  The user the Application Server, for example ″Default Server″, is running must have the following line in the `.profile`, namely,

  ```
  . /usr/lpp/cmb/ikf/IST/bin/ISTSingleWorkstationEnv.sh
  ```
- For Solaris:

  The user the Application Server, for example ″Default Server″, is running must have the following line in the `.profile`, namely,

  ```
  . /opt/IBMcmb/ikf/IST/bin/ISTSingleWorkstationEnv
  ```

8. Deploy the IST via the Administrative Console. The necessary steps are:
   - From the console menu, select **Console→Wizards→Install Enterprise Application**
   - In the panel that is displayed:
     – Select ″Install stand-alone module″
     – Select **Browse** and locate the file `IST.war` at:
       - For Windows: `<cmbroot>\ikf\IST`
       - For AIX: `/usr/lpp/cmb/ikf/IST`
       - For Solaris: `/opt/IBMcmb/ikf/IST`
     – For ″Application Name″, enter `IST`
     – For ″Context Root for Web Module″, enter `<WebPath>`, for example `/webApps/IST` Ensure that `<WebPath>` ends in `/IST`
     – Click **Next**
   - Bypass the following panels by clicking **Next**:
     – ″Mapping users to roles″
     – ″Mapping EJBRunAs Roles to Users″
     – ″Binding Enterprise Beans to JNDI names″
     – ″Mapping EJP References to Enterprise Beans″
     – ″Mapping Resource References to Resources″

  - ″Specifying the Default Datasource for EJB Modules″
  - ″Specifying Data Sources for individual CMP beans″
- In panel ″Selecting Virtual Hosts for Webmodules″, select the virtual host desired and click **Next**
- In panel ″Selecting Application Servers″, select the application server desired and click **Next**
- In the panel that is displayed, click **Finish**

9. IST uses an EIP database named `icmnlsdb`

   If your database name is different:

   - Switch to the directory where the IST is deployed, typically at `<WAS_HOME>\installedApps`
   - Switch to the directory `IST.ear/IST.war/WEB-INF` and open the file `web.xml`
   - Search for `icmnlsdb` and rename to your EIP database.
   - Save the file.
10. Restart the Application Server.
11. Re-generate the Web server plug-in configuration by:
    - In the Administrative Console, selecting **Nodes⟶<Node>⟶Application Server⟶<AppServer>**
    - Right-clicking on <AppServer> and selecting ″Regen Web Server Plugin″
12. The URL to access the Information Structuring Tool is `http://host_alias/WebPath/login.html` where:
    - `host_alias` is one of the aliases specified for `VirtualHost`. To find this value:
      - Open the WAS Administrator's Console
      - From the console menu, select **Virtual Hosts⟶<VirtualHost>⟶Aliases**
      - Each entry in the list (Host Name and Port) is a valid host alias, for example, `prefix:9080`
    - `<WebPath>` you specified during installation, for example, `/webApps/IST`

WAS V5

These instructions apply to both WAS 5 Base and WAS 5 Network Deployment (ND). For WAS 5 Network Deployment, perform steps 3 and 4 from the workstation where either the information mining feature (single workstation scenario) or the Enterprise Information Portal client (client-server setup) is installed.

After installing the WAS V5 and Enterprise Information Portal, carry out the following:

1. Start the application server
2. WAS 5 ND only: Make sure the deployment manager is started.
3. Set up a shared library in WAS with the necessary environment settings:
   - For Windows:
     - In a command shell, change to the directory `<WAS_HOME>\bin`
     - Enter `<CMBROOT>\ikf\IST\bin\SetupIMEnv <Cell> <Node> <AppServer>`, for example, for WAS V5 Base `d:\cmbroot\ikf\IST\bin\SetupIMEnv prefix prefix server1`, and for WAS V5 ND `d:\cmbroot\ikf\IST\bin\SetupIMEnv runner prefix server1`
   - For AIX:
     - In a command shell, change to the directory `<WAS_HOME>/bin`
     - Enter `/usr/lpp/cmb/ikf/IST/bin/SetupIMEnv.sh <Cell> <Node> <AppServer>`
   - For Solaris:
     - In a command shell, change to the directory `<WAS_HOME>/bin`
     - Enter `/opt/IBMcmb/ikf/IST/bin/SetupIMEnv.sh <Cell> <Node> <AppServer>`
     -
4. Deploy the IST via the Administrative Console. The necessary steps are:
   - Launch the Administrative Console browser.
   - In the Navigation Bar, select **Applications**→**Install New Application**
   - Under **Path** and browse for file `IST.war`:
     - For Windows at: `<cmbroot>\ikf\IST`
     - For AIX at: `/usr/lpp/cmb/ikf/IST`
     - For Solaris at: `/opt/IBMcmb/ikf/IST`
   - For ″Context Root″, enter `<WebPath>`, for example `/webApps/IST` Ensure that `<WebPath>` ends in `/IST`
   - Click **Next**
   - Under ″Virtual Host″, verify that ″Default virtual host name for web modules″ is checked and set to the desired virtual host
   - Click **Next**
   - Click **Next** to bypass ″ Install New Application″, Step 1
   - In ″Install New Application″, Step 2:
     - Make sure that the correct virtual host is specified
     - Click **Next**
   - Click **Next** to bypass ″ Install New Application″, Step 3
   - In ″ Install New Application″, Step 4, click **Finish**

- In the menu bar, click **Save**
- In the navigation bar, select **Applications⟶Enterprise Applications**
- Select `IST_war`
- On the **Configuration** tab, go to ″General Properties″, and uncheck ″Enable Distribution″ and ″Reload Enabled″
- Select **Apply**
- Select ″Libraries″ under ″Additional Properties″
- Click **Add**
- Select ″InformationMiningEnvironment″ from the drop-down list, then **OK**
- In the menu bar, click **Save** to save your settings

5. Update the Web server plugin configuration:
   - In the navigation bar, select **Environment⟶Update Web Server Plugin**
   - Select **OK**
6. Stop the Application Server
7. After deployment,
   - Open a command shell
   - Switch to the IST source directory at:
     - For Windows: `<CMBROOT>\ikf\IST\bin`
     - For AIX: `/usr/lpp/cmb/ikf/IST/bin`
     - For Solaris: `/opt/IBMcmb/ikf/IST/bin`
   - At the command prompt, enter:
     - For Windows: `ISTconfig <WAS_HOME> <Node>` and press **Enter**. If `WAS_HOME` contains spaces, use quotes, for example, `ISTConfig "c:\Program Files\WebSphere\AppServer" prefix`

       In Windows 2000, if you are prompted three times whether files should be replaced, enter **y** each time
     - For AIX: `./ISTconfig.sh <Node>` and press **Enter**
     - For Solaris: `./ISTconfig <Node>` and press **Enter**
8. The IST uses an EIP database named `icmnlsdb`

   If your database name is different:
   - Switch to the directory where the IST is deployed, typically at `<WAS_HOME>\installedApps\<Node>`, for example `d:\WebSphere\Appserver\installedApps\prefix`
   - Switch to the directory `IST_war.ear/IST.war/WEB-INF` and open the file `web.xml`
   - Search for `icmnlsdb` and rename to your EIP database.
   - Save the file.

9. Restart the Application Server.
10. The URL to access the Information Structuring Tool is `http://host_alias/WebPath/login.html` where:
    - `host_alias` is one of the aliases specified for `VirtualHost`. To find this value:
      - Open the WAS Administrator's Console
      - From the navigation panel, select **Environment⟶Virtual Hosts⟶<VirtualHost>⟶Host Aliases**

        Each entry in the list (Host Name and Port) is a valid host alias, for example, `prefix:9080`
    - `<WebPath>` you specified during installation, for example, `/webApps/IST`

Browser settings

Browser langauge setting

The language used in the Information Structuring Tool GUI is determined by the language settings of the Web browser you are using. To change these settings:

- For the Internet Explorer:
  - Select **Tools⟶Internet Options⟶Languages** from the menu bar
  - Select your preferred language from the list
  - Click **Move Up** to list the language at the top
- For Netscape:
  - Select **Edit⟶Preferences⟶Navigator⟶Languages** from the menu bar
  - Select **Add** to add a language
  - Select your preferred language from the list and move it to the top of the list

Access the Information Structuring Tool in your selected langauge using the .../IST/login.html page.

Cache settings

The recommended Web browser cache settings are the following:

- For the Internet Explorer:
  - Select **Tools⟶Internet Options—** from the menu bar
  - Under ″Temporary Internet Files″, select ″Settings″
  - Under ′Check for newer versions of stored pages″, select ″Every visit to the page″
- For Netscape:
  - Select **Edit⟶Preferences⟶Advanced⟶Cache** from the menu bar

- Under ″Document in cache is compared to the network″, select ″Every time″

Cookies and Javascript

To use the Information Structuring Tool, both cookies and Javascript must be enabled in the browser.

Configuring the Web Application Server for the JSP sample

Before you can install the JSPs on the Websphere Application Server Advanced Edition (WAS 4 AE) or Advanced Edition Single Server (WAS 4 AEs), or the Websphere Application Server 5 Base or the Websphere Application Server 5 Network Deployment (ND), you need the following information:

- `<Node>` is the name of the workstation where the JSPs are to be installed.
- `<AppServer>` is the Application Server on `<Node>` where the JSPs are to be installed, for example, `Default Server` for WAS 4 and `server1` for WAS 5.
- `<VirtualHost>` is the name of the virtual host the JSPs are to run on, for example, `default_host`
- `<WebPath>` is the path portion of the URL used to access the JSPs. For example, if the JSPs are installed on the server `prefix` and `<WebPath>` is `/miningSamples`, the URL to access the JSPs is `http://prefix:9080/miningSamples/logon.html`
- `<WAS_HOME>` is the directory where the WAS is installed on `<Node>`, for example, `d:\WebSphere\AppServer` on Windows, `/usr/WebSphere/AppServer` on AIX and on Solaris, `/opt/WebSphere/AppServer`.
- WAS 5 only: `<Cell>` is the name of the administrative cell. For WAS 5 Base, this is the same as `<Node>`. For WAS 5 ND, this is the name of the workstation the deployment manager is running on.
- For Windows:
  - `<CMBROOT>` is the value of the corresponding environment variable, for example, `d:\cmbroot`
  - `<DB2HOME>` is the value of the corresponding environment variable, for example, `d:\sqllib`
- For AIX:
  - `<DB2HOME>` is the directory where DB2 is installed, for example, `/usr/lpp/db2_07_01` or `/usr/opt/db2_08_01`

    `<DB2JAVAHOME>` is the directory where the Java 1.2 library files are located. For DB2 V7, this is `<DB2HOME>/java12` and for DB2 V8, `<DB2HOME>/java`
- For Solaris:
  - `<DB2HOME>` is the directory where DB2 is installed, for example, `/opt/IBMdb2/V7.1` or `/opt/IBMdb2/V8.1`

`<DB2JAVAHOME>` is the directory where the Java 1.2 library files are located. For DB2 V7, this is `<DB2HOME>/java12` and for DB2 V8, `<DB2HOME>/java`

We recommend that you deploy the JSPs on the same application server you deployed the Information Structuring Tool on. If you do, then you can continue deploying the JSPs at step 7 for WAS AEs or WAS AE. If the JSPs are not deployed on the same application server, refer to “Installation scenarios” on page 460 before continuing with the following sections.

WAS V4

The following section describes the IST deployment procedure in WAS 4 AEs, followed by WAS 4 AE.

WAS AEs: After installing the WAS AEs and Enterprise Information Portal, open the WAS Administrator’s Console and carry out the following:

1. From the console menu, select **Nodes→<Node>→Application Server→<AppServer>→Process Definitions→JVM Settings**
2. If the WAS and Enterprise Information Portal are on the same workstation, enter the following `Classpath` information:
   - For Windows:

     ```
     <CMBROOT>\ikf\lib
     <CMBROOT>\ikf\lib\ikf.jar
     <CMBROOT>\lib\cmb81.jar
     <CMBROOT>\lib\cmbsdk81.jar
     <CMCOMMON>
     <CMBROOT>\lib\cmblog4j81.jar
     <CMBROOT>\lib\log4j.jar
     <DB2HOME>\java\db2java.zip
     ```
   - For AIX:

     ```
     /usr/lpp/cmb/ikf/lib
     /usr/lpp/cmb/ikf/lib/ikf.jar
     /usr/lpp/cmb/lib
     /usr/lpp/cmb/lib/cmb81.jar
     /usr/lpp/cmb/lib/cmbsdk81.jar
     /usr/lpp/cmb/cmgmt
     /usr/lpp/cmb/lib/cmblog4j81.jar
     /usr/lpp/cmb/lib/log4j.jar
     <DB2JAVAHOME>/db2java.zip
     ```
   - For Solaris:

     ```
     /opt/IBMcmb/ikf/lib
     /opt/IBMcmb/ikf/lib/ikf.jar
     /opt/IBMcmb/lib
     /opt/IBMcmb/lib/cmb81.jar
     /opt/IBMcmb/lib/cmbsdk81.jar
     /opt/IBMcmb/cmgmt
     /opt/IBMcmb/lib/cmblog4j81.jar
     /opt/IBMcmb/lib/log4j.jar
     <DB2JAVAHOME>/db2java.zip
     ```

If the WAS and Enterprise Information Portal are on different workstations, the `Classpath` information is as follows:

- For Windows:

  ```
  <CMBROOT>\ikf\lib\ikf.jar
  <CMCOMMON>
  <CMBROOT>\lib\cmb81.jar
  ```

- For AIX:

  ```
  /usr/lpp/cmb/ikf/lib/ikf.jar
  /usr/lpp/cmb/cmgmt
  /usr/lpp/cmb/lib/cmb81.jar
  ```

- For Solaris:

  ```
  /opt/IBMcmb/ikf/lib/ikf.jar
  /opt/IBMcmb/lib/cmgmt
  /opt/IBMcmb/lib/cmb81.jar
  ```

3. Select **OK** at the bottom of the page.
4. Save your configuration settings by clicking **Save** on the top bar of the WAS administrative console.
5. If the WAS and Enterprise Information Portal are on the same workstation:
   - For Windows:

     The PATH must be set in the WAS Administrative Console:

     - From the console menu, select **Nodes→<Node>→Application Server→<AppServer>→Process Definitions**
     - Under ″Advanced Settings″, select ″Environment″
     - In ″System Properties″, select ″New″
     - For ″property name″, enter PATH and for ″property value″, enter `<cmbroot>\ikf\bin`, for example, `d:\cmbroot\ikf\bin`
     - Select **OK**
     - Select **Save** on the top bar of the WAS administrative console
   - For AIX:

     The user who starts the Application Server, for example ″root″, must have the following line in the `.profile`, namely,

     ```
     . /usr/lpp/cmb/ikf/IST/bin/ISTSingleWorkstationEnv.sh
     ```
   - For Solaris:

     The user who starts the Application Server, for example ″root″, must have the following line in the `.profile`, namely,

     ```
     . /opt/IBMcmb/ikf/IST/bin/ISTSingleWorkstationEnv
     ```
6. Click **Exit** on the top bar of the console to exit.
7. Shut down the WAS by:
   - Switching to the directory `<WAS_Home>\bin` in a command shell
   - Entering:

   - For Windows: `stopserver`
   - For AIX: `./stopServer.sh`
   - For Solaris: `./stopServer.sh`
8. In the command shell, enter:
   - For Windows: `seappinstall -install <CMBROOT>\samples\jsp\infomining\jsp.war`
   - For AIX: `./SEAppInstall.sh -install /usr/lpp/cmb/samples/jsp/infomining/jsp.war`
   - For Solaris: `./SEAppInstall.sh -install /opt/IBMcmb/samples/jsp/infomining/jsp.war`

   You are prompted as follows:
   - Please specify an application display name: Enter `InfoMiningSamples`
   - Please specify a context root: Enter your `<WebPath>`, for example, `/webApps/IST` Ensure that `<WebPath>` ends in `/IST`
   - Do you wish to precompile all JSPs in this application: Enter `n`
   - Do you wish to precompile individual Web Applications: Enter `n`
   - Please specify a virtual host for the following Web applications, IBM information mining Samples JSPs: Enter your `<VirtualHost>`, for example `default_host`
9. Restart the WAS in the command shell by entering:
   - For Windows: `startserver`
   - For AIX: `./startServer.sh`
   - For Solaris: `./startServer.sh`
10. Re-generate the Web server plug-in configuration of WAS by:
    - Opening the Administrative Console
    - Selecting **Nodes→<Node>→Application Server→<AppServer>**
    - Under ″Advanced Settings″, selecting ″Web Server Plugin Configuration″
    - Selecting ″Generate″
11. The URL to access the JSPs is `http://host_alias/WebPath/logon.html` where:
    - `host_alias` is one of the aliases specified for `VirtualHost`. To find this value:
      - Open a WAS Administrator's Console
      - From the console menu, select **Virtual Hosts→<VirtualHost>→Aliases**
      - Each entry in the list (Host Name and Port) is a valid host alias, for example, `prefix:9080`

- <WebPath> you specified during installation, for example, /webApps/JSPs

WAS AE: After installing the WAS AE and Enterprise Information Portal, open the WAS Administrator's Console and carry out the following:

1. On the console menu, select **Nodes—►<Node>—►Application Server—►<AppServer>**
2. Stop the Application Server, if it is running.
3. Select the tab **JVM Settings** on the right.
4. If the WAS and Enterprise Information Portal are on the same workstation, enter the following Classpath information:
   - For Windows:
     ```
     <CMBROOT>\ikf\lib
     <CMBROOT>\ikf\lib\ikf.jar
     <CMBROOT>\lib\cmb81.jar
     <CMBROOT>\lib\cmbsdk81.jar
     <CMCOMMON>
     <CMBROOT>\lib\cmblog4j81.jar
     <CMBROOT>\lib\log4j.jar
     <DB2HOME>\java\db2java.zip
     ```
   - For AIX:
     ```
     /usr/lpp/cmb/ikf/lib
     /usr/lpp/cmb/ikf/lib/ikf.jar
     /usr/lpp/cmb/lib
     /usr/lpp/cmb/lib/cmb81.jar
     /usr/lpp/cmb/lib/cmbsdk81.jar
     /usr/lpp/cmb/cmgmt
     /usr/lpp/cmb/lib/cmblog4j81.jar
     /usr/lpp/cmb/lib/log4j.jar
     <DB2JAVAHOME>/db2java.zip
     ```
   - For Solaris:
     ```
     /opt/IBMcmb/ikf/lib
     /opt/IBMcmb/ikf/lib/ikf.jar
     /opt/IBMcmb/lib
     /opt/IBMcmb/lib/cmb81.jar
     /opt/IBMcmb/lib/cmbsdk81.jar
     /opt/IBMcmb/cmgmt
     /opt/IBMcmb/lib/cmblog4j81.jar
     /opt/IBMcmb/lib/log4j.jar
     <DB2JAVAHOME>/db2java.zip
     ```

   If the WAS and Enterprise Information Portal are on different workstations, the Classpath information is as follows:

   – For Windows:
     ```
     <CMBROOT>\ikf\lib\ikf.jar
     <CMCOMMON>
     <CMBROOT>\lib\cmb81.jar
     ```
   – For AIX:

```
/usr/lpp/cmb/ikf/lib/ikf.jar
/usr/lpp/cmb/cmgmt
/usr/lpp/cmb/lib/cmb81.jar
```

   – For Solaris:

```
/opt/IBMcmb/ikf/lib/ikf.jar
/opt/IBMcmb/cmgmt
/opt/IBMcmb/lib/cmb81.jar
```

5. Select **Apply** at the bottom of the page.
6. If the WAS and Enterprise Information Portal are on the same workstation:
   - For Windows:

     The server the IST is deployed in must contain an additional PATH entry:

     – From the console menu, select **Nodes→<Node>→Application Server→<AppServer>**

     – In the ″General″ tab, select ″Environment...″

     – In the Environment Editor frame, select ″Add″

     – For ″Name″, enter PATH and for ″Value″, enter `<cmbroot>\ikf\bin`, for example, `d:\cmbroot\ikf\bin`

     – Select **OK**

     – Select **Apply**
   - For AIX:

     The user the Application Server, for example ″Default Server″, is running under must have the following line in the `.profile`, namely,

     ```
     . /usr/lpp/cmb/ikf/IST/bin/ISTSingleWorkstationEnv.sh
     ```
   - For Solaris:

     The user the Application Server, for example ″Default Server″, is running under must have the following line in the `.profile`, namely,

     ```
     . /opt/IBMcmb/ikf/IST/bin/ISTSingleWorkstationEnv
     ```
7. Deploy the JSPs via the Administrative Console. The necessary steps are:
   - From the console menu, select **Console→Wizards→Install Enterprise Application**
   - In the panel that is displayed:

     – Select ″Install stand-alone module″

     – Select **Browse** and locate the file `jsp.war` at:

       - For Windows: `<cmbroot>>\samples\jsp\infomining`
       - For AIX: `/usr/lpp/cmb/samples/jsp/infomining`
       - For Solaris: `/opt/IBMcmb/samples/jsp/infomining`

     – For ″Application Name″, enter `InfoMiningSamples`

  - For ″Context Root for Web Module″, enter `<webPath>`, for example `/webApps/InfoMiningSamples`
  - Click **Next**
- Bypass the following panels by clicking **Next**:
  - ″Mapping users to roles″
  - ″Mapping EJBRunAs Roles to Users″
  - ″Binding Enterprise Beans to JNDI names″
  - ″Mapping EJP References to Enterprise Beans″
  - ″Mapping Resource References to Resources″
  - ″Specifying the Default Datasource for EJB Modules″
  - ″Specifying Data Sources for individual CMP beans″
- In panel ″Selecting Virtual Hosts for Webmodules″, select the virtual host desired and click **Next**
- In panel ″Selecting Application Servers″, select the application server desired and click **Next**
- In the panel that is displayed, click **Finish**

8. Restart the Application Server in the console.
9. Re-generate the Web server plug-in configuration by:
   - In the Administrative Console, selecting **Nodes⟶<Node>⟶Application Server⟶<AppServer>**
   - Right-clicking on <AppServer> and selecting ″Regen Web Server Plugin″
10. The URL to access the JSPs is `http://host_alias/WebPath/logon.html` where:
    - `host_alias` is one of the aliases specified for `VirtualHost`. To find this value:
      - Open the WAS Administrator's console
      - From the console menu, select **Virtual Hosts⟶<VirtualHost>⟶Aliases**
      - Each entry in the list (Host Name and Port) is a valid host alias, for example, `prefix:9080`
    - `<WebPath>` you specified during installation, for example, `/miningSamples`

WAS V5

If you deploy the Sample JSPs on the same `<Cell>` as the Information Structuring Tool, you can skip step 3.

These instructions apply to both WAS 5 Base and WAS 5 Network Deployment (ND). For WAS 5 Network Deployment, perform steps 3 and 4 from the workstation where either the information mining feature (single workstation scenario) or the Enterprise Information Portal client (client-server setup) is installed.

After installing the WAS V5 and Enterprise Information Portal, carry out the following:

1. Start the application server
2. WAS 5 ND only: Make sure the deployment manager is started.
3. Set up a shared library in WAS with the necessary environment settings:
   - For Windows:
     - In a command shell, change to the directory `<WAS_Home>\bin`
     - Enter `<CMBROOT>\ikf\IST\bin\SetupIMEnv <Cell> <Node> <AppServer>`, for example, for WAS V5 Base `d:\cmbroot\ikf\IST\bin\SetupIMEnv prefix prefix server1`, and for WAS V5 ND `d:\cmbroot\ikf\IST\bin\SetupIMEnv runner prefix server1`
   - For AIX:
     - In a command shell, change to the directory `<WAS_Home>/bin`
     - Enter `/usr/lpp/cmb/ikf/IST/bin/SetupIMEnv.sh <Cell> <Node> <AppServer>`
   - For Solaris:
     - In a command shell, change to the directory `<WAS_Home>/bin`
     - Enter `/opt/IBMcmb/ikf/IST/bin/SetupIMEnv.sh <Cell> <Node> <AppServer>`
     -
4. Deploy the JSPs via the Administrative Console. The necessary steps are:
   - Launch the Administrative Console browser.
   - In the Navigation Bar, select **Applications→Install New Application**
   - Under **Path** and browse for file `JSP.war`:
     - For Windows at: `<cmbroot>\samples\jsp\infomining`
     - For AIX at: `/usr/lpp/cmb/samples/jsp/infomining`
     - For Solaris at: `/opt/IBMcmb/samples/jsp/infomining`
   - For ″Context Root″, enter `<WebPath>`, for example `/webApps/InfoMiningSamples`
   - Click **Next**
   - Under ″Virtual Host″, verify that ″Default virtual host name for web modules″ is checked and set to the desired virtual host
   - Click **Next**
   - Click **Next** to bypass ″ Install New Application″, Step 1

- In ″Install New Application″, Step 2:
  - Make sure that the correct virtual host is specified
  - Click **Next**
- Click **Next** to bypass ″ Install New Application″, Step 3
- In ″ Install New Application″, Step 4, click **Finish**
- In the menu bar, click **Save**
- In the navigation bar, select **Applications⟶Enterprise Applications**
- Select `jsp.war`
- On the **Configuration** tab, go to ″General Properties″, and uncheck ″Enable Distribution″
- Select **Apply**
- Select ″Libraries″ under ″Additional Properties″
- Click **Add**
- Select ″InformationMiningEnvironment″ from the drop-down list, then **OK**
- In the menu bar, click **Save** to save your settings

5. Update the Web server plugin configuration:
   - In the navigation bar, select **Environment⟶Update Web Server Plugin**
   - Select **OK**
6. Stop the Application Server
7. Restart the Application Server.
8. The URL to access the JSPs is `http://host_alias/WebPath/login.html` where:
   - `host_alias` is one of the aliases specified for `VirtualHost`. To find this value:
     - Open the WAS Administrator's Console
     - From the navigation panel, select **Environment⟶Virtual Hosts⟶<VirtualHost>⟶Host Aliases**

       Each entry in the list (Host Name and Port) is a valid host alias, for example, `prefix:9080`
   - `<WebPath>` you specified during installation, for example, `/webApps/InfoMiningSamples`

Chapter 32. Using Content Manager after-install programs and procedures

This section describes the programs and procedures that may be used at any time after the Content Manager components have been installed. Programs and procedures described in this section include:

- "Starting the information center"
- "Migrating to Content Manager Version 8 from a previous version"
- "Enabling LDAP" on page 482
- "Utility programs for creating or replacing databases" on page 487
- "Deploying and configuring the resource manager with WAS Advanced Edition (AE)" on page 496
- "Running the server configuration utility program" on page 498
- "Running the library server monitor program" on page 498
- "Running the First Steps program" on page 499
- "Installing and configuring IBM License Use Management (LUM)" on page 500
- "Uninstall procedures" on page 503

Starting the information center

The information center includes the documentation for Content Manager, Enterprise Information Portal, and IBM Content Manager VideoCharger. Topic-based information is organized by product and by task (for example, Administration). In addition to the provided navigation mechanism and indexes, a search facility also aids retrievability.

To start the information center, click **Start** → **Program Files** → **IBM Content Manager for Multiplatforms V8.2** → **Information center**.

Migrating to Content Manager Version 8 from a previous version

See the *Migrating to Content Manager Version 8* for the information that you need to plan for and migrate Content Manager data and applications. It provides guidelines, recommendations, and detailed steps for various migration scenarios.

Enabling LDAP

During the installation of Content Manager, you are given the opportunity to Enable LDAP. If you do not enable LDAP during installation, you can still enable it at any time.

Content Manager supports importing of users and user authentication using the standard LDAP protocols, from the following:

- IBM Directory Server (previous versions were called IBM Secureway Directory)
- Lotus Domino Directory Notes Address Book (NAB)
- Microsoft Active Directory

You can select IBM Directory and Domino Address Book from the installation menu as the ″Standard LDAP″ option and in the system administration client utility program as the ″LDAP″ selection.

Setting up LDAP user import and authentication after installation

This process includes five steps:

1. Generating the properties file
2. Installing the properties file
3. Installing the user exit
4. Installing prerequisite software
5. Enabling Secure Sockets Layer (SSL) for LDAP server communication (if required)

Step 1. Generating the properties file

You can enable LDAP at any time as follows:

1. Launch the system administration client
2. Click **Tools->LDAP Configuration**
3. Check the **Enable LDAP User Import and Authentication** check box
4. Click the **Server** tab
5. Fill in the LDAP server related information

When the configuration is complete, a `cmbcmenv.properties` file is generated in the directory pointed to by the CMCOMMON environment variable on the system.

Step 2. Installing the properties file

This file is used by the system administration client utility program for importing users from the LDAP server. The library server and the resource manageralso require this file for the user authentication from the LDAP server.

For the library server, continue with "Installing the properties file on the library server".

For the resource manager, see "Installing the properties file on the resource manager".

Installing the properties file on the library server: If the library server is on a different workstation than the system administration client, you need to copy the generated cmbcmenv.properties file over to the library server machine, into the directory that is pointed to by the CMCOMMON environment variable. If there are multiple library server databases installed, you might want to copy it into a directory (under CMCOMMON) with the same name as the database name. The library server LDAP user-exit looks for this properties file under a directory of the database name, which should exist under the directory pointed to by the CMCOMMON environment variable.

For example, on a Unix system, if the library server database is ICMNLSDB, then the library server looks for the cmbcmenv.properties file under the directory:

```
$CMCOMMON/ICMNLSDB
```

Similarly on a Windows machine, it looks under the directory:

```
%CMCOMMON%/ICMNLSDB
```

Copy the properties file into this directory with the matching name of the library server database as described above. If there are multiple library server databases installed on the same machine, this is the recommended place for the properties file.

If the properties file is not found in the directory with the database name under CMCOMMON, the library server then looks for the file under the directory pointed to by CMCOMMON.

Installing the properties file on the resource manager: For the resource manager, you need to copy the generated cmbcmenv.properties file over to the resource manager:

1. Copy the cmbcmenv.properties file to the following directory:

   ```
   <WAS_HOME>\installedApps\icmrm.ear\icmrm.war\WEB-INF\classes
   \com\ibm\mm\<icmrm>
   ```

   Where: <icmrm> is the resource manager application name (the install default name).
2. Edit the cmbcmenv.properties file in the above directory and change all encrypted passwords to clear text passwords. (When you restart the server, the passwords will be re-encrypted.)
3. Restart the server.

If you are not using WebSphere, you need to put the ibmjsse.jar file in your classpath.

Important: The change password request in the LDAP server is not supported. You must use the LDAP server's administrative tool (for example: the Directory Management tool of IBM Directory) to change the password yourself.

Step 3. Installing the user exit

A directory by the name of **ldap**, containing the ICMXLSLG.DLL user-exit, resides under the directory pointed to by the ICMROOT environment variable.

On a Windows workstation

Copy the ICMXLSLG.DLL LDAP User-exit DLL from this directory into the %ICMROOT%/<DBNAME>/DLL directory.

On a Unix workstation

1. Copy the ICMXLSLG.DLL LDAP User-exit DLL from this directory into the $ICMDLL/<DBNAME>/DLL directory. **Important:** when copying the ICMXLSLG.DLL, remember to preserve the uppercase characters in its name.
2. Set the permission on the copied DLL. For example, if the <DBNAME> is ICMNLSDB:

```
cd $ICMDLL
    cd ICMNLSDB/DLL
    cp $ICMROOT/ldap/ICMXLSLG.DLL .
    chmod 555 ICMXLSLG.DLL
```

Very important:

- Never edit the cmbcmenv.properties file. Always use the system administration client utility program to make any changes and then copy and install the updated cmbcmenv.properties file onto the library server machine.
- Make sure that the .profile for the icmadmin user and the /home/$DB2INSTANCE/sqllib/db2profile have been updated for the CMCOMMON environment variable as directed by the procedure (beginning with) step 3 on page 248 for AIX, or (beginning with) step 3 on page 358 for Solaris.

Step 4. Installing prerequisite software for LDAP user authentication

Two prerequisite programs are required for LDAP user authentication:

- IBM Directory client/SDK
- Global Security Kit (GSKit) Version 5 (if you are planning to use Secure Sockets Layer (SSL) with your LDAP user authentication)

For specific installation instructions, see the IBM Directory installation and configuration guide (included with the package on the documentation CD).

IBM Directory client SDK

- On a Windows machine, insert the IBM Directory CD. Follow directions to install the `client SDK`.
- On an AIX machine, select and install as follows:
  - Select `ldap.client` if you do not plan to use SSL
  - If you do plan to use SSL, select `ldap.max_crypto_client` instead
- On a Solaris machine, select IBM Directory Client (IBMldapc)

Global Security Kit (GSKit) Version 5

If you plan to use Secure Sockets Layer (SSL), you must also install the Global Security Kit (GSKit) on the library server machine.

The GSKit software is provided on the IBM Directory server CD. Install the software as follows:

- On a Windows machine, run `setup.exe` from the `gskit` directory.
- On an AIX machine, install the program using `gskkm.rte` under the `gskit` directory
- On a Solaris machine, install the Certificate and SSL Base Runtime (`gsk5bas`) from under the `gskit` directory

Step 5. Enabling SSL for LDAP server communication

There are four steps required for configuring SSL for LDAP user authentication:

1. Creating the key database file (.kdb)
2. Configuring the system administration client for SSL communication
3. Configuring the library server for SSL communication with the LDAP server
4. Configuring the resource manager for SSL communication with the LDAP server

Creating the key database file: The LDAP server must be configured for SSL using the Server Authentication method only. (The Server and Client Authentication method is not supported.)

Use the following procedure to create the key database file:

1. Export the SSL certificate from the LDAP server in either Base64-encoded ASCII data or Binary Der data formats
2. Start the `ikeyman` utility.

   You can start this utility from either one of the following:

   - GSKit software (`gsk5ikm.exe`)

- The IBM HTTP server

3. From the Key Database File menu, select **New**
4. As a **key database type**, enter: `CMS key database file`
5. In the **File Name** field, enter a name for your key database file (for example:`ldapkey.kdb`)
6. In the **Location** field, enter: `c:\Program Files\IBM\CMGMT` (or any location on the local disk)
7. Click **OK**
8. Enter a password
9. In the Signer Certificates panel, click **Add**
10. Fill in the name and location of the previously exported LDAP SSL certificate
11. Click **OK**
12. Copy the generated `<ldapkey_name>.kdb` file into the directory pointed to by the CMCOMMON environment variable on the library server machine.

Configuring the system administration client for SSL communication: Follow these steps to configure the system administration client for SSL:

1. Start the system administration client (**Start** → **Programs** → **IBM Content Manager for Multiplatforms V8.2** → **System Administration**)
2. Click **Tools** → **LDAP configuration**
3. From the Authentication panel, check the **Secure Sockets Layer** selection box
4. Enter the name of the key database file that you created during "Creating the key database file" on page 485 (for example: `ldapkey`). **Important:** do not add the `.kdb` extension to the file name in this field.
5. Enter the SSL authentication password in the **Password** field. (Enter the password that you used during "Creating the key database file" on page 485.)
6. Click **OK**. (This updates the `cmbcmenv.properties` file in the directory pointed to by the CMCOMMON environment variable.) If the library server is on a different machine than the system administration client, you need to copy the `cmbcmenv.properties` file over to the library server during "Configuring the library server for SSL communication with the LDAP server" on page 487.
7. Launch the Java Runtime Environment (JRE) `ikeyman` utility program from the `jdk/jre/bin` directory, to open the `cacerts` file.

   You can locate the `jdk/jre/bin` directory as follows:

   - If Enterprise Information Portal is installed on this system, navigate to the file in this location:

`%CMBROOT%/jdk/jre/lib/security/cacerts`

- If Enterprise Information Portal is not installed on this system (only Content Manager), navigate to the file in this location:

  `%ICMROOT%/jdk/jre/lib/security/cacerts.`

8. Enter the password. (If the file has not been changed, the default password here is `changeit`.
9. Add the exported SSL LDAP certificate into the `cacerts` file.
10. Restart the system administration client and launch **Import users from LDAP** from the New User panel. It should now be able to communicate with the LDAP server over SSL.

Configuring the library server for SSL communication with the LDAP server: If the library server is on a different machine than the system administration client, you have two additional steps to perform:

1. Copy the `cmbcmenv.properties` file (updated with the SSL information) from the system administration client machine to the library server machine (as explained earlier in"Installing the properties file on the library server" on page 483.
2. Copy the key database file (`ldapkey.kdb`), generated during "Creating the key database file" on page 485, into the directory pointed to by the CMCOMMON environment variable.

Configuring the resource manager for SSL communication with the LDAP server: To configure the resource manager for SSL communication with the LDAP server, you have three additional steps to perform:

1. Follow the same procedure for installing the `cmbcmenv.properties` file (updated with the SSL information) from the system administration client to the resource manager (as explained earlier in "Installing the properties file on the resource manager" on page 483.
2. Add the exported SSL LDAP certificate into the following file:

   `<WAS_HOME>\java\jre\lib\security\cacerts`
3. Restart the server.

Utility programs for creating or replacing databases

This section describes how to create or replace the following databases on a Content Manager (CM) or an Enterprise Information Portal (EIP) system:

- A Content Manager DB2 library server database
- A Content Manager DB2 resource manager database
- An Enterprise Information Portal DB2 system administration database
- A Content Manager Oracle library server database
- A Content Manager Oracle resource manager database

Before you begin to use these utility programs, you need to make sure that you know about database ″administration″ and/or ″connection″ user IDs (if they do not already exist) for use during these utility programs. These user IDs were probably created before your original installation of Content Manager or Enterprise Information Portal.

For more information about the user IDs, refer to the section that applies to your operating system as follows:

For the Windows operating system
See "Create user IDs with the proper user rights and privileges" on page 99.

For the AIX operating system
See "Create user IDs" on page 235.

For the Solaris operating system
See "Create user IDs" on page 345.

See Table 167 to continue with instructions for creating the specific database:

Table 167. Database creation utility program

"Creating or replacing a CM DB2 library server database" in the next section
"Creating or replacing a CM DB2 resource manager database" on page 490
"Creating or replacing an EIP DB2 system administration database" on page 491
"Creating or replacing a CM Oracle library server database" on page 492
"Creating or replacing a CM Oracle resource manager database" on page 494

Creating or replacing a CM DB2 library server database

This section describes the utility program that is used to create or replace a Content Manager DB2 library server database. During the process, the program checks to see if either a CM library server database or an EIP system administration database already exists on the workstation. If either one exists, the program asks you questions to help you decide whether to replace the database, or to create a new database with a new name. You cannot have two databases on the same workstation with the same name.

To start the utility program to create or replace a library server database:

On a Windows system

1. Open the Command Prompt window
2. Navigate to the Content Manager directory (%icmroot%\config\), for example:

   ```
   c:\Program Files\ibm\Cm81\Config\
   ```
3. Enter the command

```
icmcreatelsdb
```

4. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.
5. **Very important:** After you create a new library server database, remember to update the following configuration files:

   ```
   cmbicmenv.ini
   cmbicmsrvs.ini
   ```

   See Chapter 34, "Generating configuration files", on page 515 for more information about updating configuration files.

On an AIX system

1. Navigate to the Content Manager directory (%icmdll%), for example:

   ```
   /usr/lpp/icm/Config/
   ```
2. Enter the command

   ```
   icmcreatelsdb.sh
   ```

   Requirement: This command is case-sensitive. Enter it exactly as shown (lowercase).
3. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.
4. **Very important:** After you create a new library server database, remember to update the following configuration files:

   ```
   cmbicmenv.ini
   cmbicmsrvs.ini
   ```

   See Chapter 34, "Generating configuration files", on page 515 for more information about updating configuration files.

On a Solaris system

1. Navigate to the Content Manager directory (%icmdll%), for example:

   ```
   /opt/IBMicm/Config/
   ```
2. Enter the command

   ```
   icmcreatelsdb.sh
   ```

   Requirement: This command is case-sensitive. Enter it exactly as shown (lowercase).
3. Follow the instructions provided by the utility program.

Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.

4. **Very important:** After you create a new library server database, remember to update the following configuration files:

   ```
   cmbicmenv.ini
   cmbicmsrvs.ini
   ```

   See Chapter 34, "Generating configuration files", on page 515 for more information about updating configuration files.

Creating or replacing a CM DB2 resource manager database

To start the utility program to create or replace a DB2 resource manager database:

On a Windows system

1. Open the Command Prompt window
2. Navigate to the Content Manager directory (%icmroot%\config\), for example:

   ```
   c:\Program Files\ibm\Cm81\Config\
   ```
3. Enter the command

   ```
   icmcreatermdb
   ```
4. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.

On an AIX system

1. Navigate to the Content Manager directory (%icmdll%), for example:

   ```
   /usr/lpp/icm/Config/
   ```
2. Enter the command

   ```
   icmcreatermdb.sh
   ```

   Requirement: This command is case-sensitive. Enter it exactly as shown (in lowercase).
3. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.

On a Solaris system

1. Navigate to the Content Manager directory (%icmdll%), for example:

   ```
   /opt/IBMicm/Config/
   ```
2. Enter the command

   ```
   icmcreatermdb.sh
   ```

Requirement: This command is case-sensitive. Enter it exactly as shown (in lowercase).

3. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.

Creating or replacing an EIP DB2 system administration database

This section describes the utility program that is used to create or replace an Enterprise Information Portal system administration database. During the process, the program checks to see if either a CM library server database or an EIP system administration database already exists on the workstation. If either one exists, the program asks you questions to help you decide whether to replace the database, or to create a new database with a new name. You cannot have two databases on the same workstation with the same name.

To start the utility program to create or replace a system administration database:

On a Windows system

1. Open the Command Prompt window
2. Navigate to the Enterprise Information Portal directory (%cmbroot%\config\), for example:

   ```
   c:\cmbroot\config\createdb\utility\
   ```
3. Enter the command

   ```
   eipcreatelsdb
   ```
4. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.
5. **Very important:** After you create a new system administration database, remember to update the following configuration files:

   ```
   cmbfedenv.ini
   cmbds.ini
   ```

   See Chapter 34, “Generating configuration files”, on page 515 for more information about updating configuration files.

On an AIX system

1. Navigate to the Content Manager directory (%cmbdll%), for example:

   ```
   /usr/lpp/cmb/config/
   ```
2. Enter the command

   ```
   eipcreatelsdb.sh
   ```

Requirement: This command is case-sensitive. Enter it exactly as shown (in lowercase).

3. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.

4. **Very important:** After you create a new system administration database, remember to update the following configuration files:

   ```
   cmbfedenv.ini
   cmbds.ini
   ```

   See Chapter 34, "Generating configuration files", on page 515 for more information about updating configuration files.

On a Solaris system

1. Navigate to the Enterprise Information Portal directory (%cmbdll%), for example:

   ```
   /opt/ibmcmb/config/
   ```

2. Enter the command

   ```
   eipcreatelsdb.sh
   ```

   Requirement: This command is case-sensitive. Enter it exactly as shown (in lowercase).

3. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.

4. **Very important:** After you create a new system administration database, remember to update the following configuration files:

   ```
   cmbfedenv.ini
   cmbds.ini
   ```

   See Chapter 34, "Generating configuration files", on page 515 for more information about updating configuration files.

Creating or replacing a CM Oracle library server database

This section describes the utility programs that are used to create or replace a Content Manager Oracle library server database. There are two utility programs:

- A create program
- A setup and load program

The two utility programs must be executed in the correct order as outlined in the steps below.

Make sure that you have met all of the prerequisites for installing an Oracle database. For details about the prerequisites, refer to the section that applies to your operating system as follows:

For the Windows operating system
See the section "Oracle database on a Windows system" on page 86.

For the AIX operating system
See the section "Oracle database on an AIX system" on page 222.

For the Solaris operating system
See the section "Oracle database on a Solaris system" on page 335.

To start the utility program to create or replace a library server database:

On a Windows system

1. Open the Command Prompt window
2. Navigate to the Content Manager directory (%icmroot%\config\), for example:
   ```
   c:\Program Files\ibm\Cm81\Config\
   ```
3. Enter the following command to create the database:
   ```
   icmcreatelsdb.ora
   ```
4. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.
5. After you create the database, enter the following command to set up and load the database you created in the previous steps:
   ```
   icmsetuplsdb.ora
   ```
6. **Very important:** After you create and set up the new library server database, remember to update the following configuration files:
   ```
   cmbicmenv.ini
   cmbicmsrvs.ini
   ```
   See Chapter 34, "Generating configuration files", on page 515 for more information about updating configuration files.

On an AIX system

1. Navigate to the Content Manager directory (%icmdll%), for example:
   ```
   /usr/lpp/icm/Config/
   ```
2. Enter the command
   ```
   icmcreatelsdb.ora.sh
   ```
   Requirement: This command is case-sensitive. Enter it exactly as shown (lowercase).

3. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.
4. After you create the database, enter the following command to set up and load the database you created in the previous steps:

   ```
   icmsetuplsdb.ora.sh
   ```
5. **Very important:** After you create and set up the new library server database, remember to update the following configuration files:

   ```
   cmbicmenv.ini
   cmbicmsrvs.ini
   ```

   See Chapter 34, "Generating configuration files", on page 515 for more information about updating configuration files.

On a Solaris system

1. Navigate to the Content Manager directory (%icmdll%), for example:

   ```
   /opt/IBMicm/Config/
   ```
2. Enter the command

   ```
   icmcreatelsdb.ora.sh
   ```

   Requirement: This command is case-sensitive. Enter it exactly as shown (lowercase).
3. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.
4. After you create the database, enter the following command to set up and load the database you created in the previous steps:

   ```
   icmsetuplsdb.ora.sh
   ```

   Requirement: This command is case-sensitive. Enter it exactly as shown (lowercase).
5. **Very important:** After you create and set up the new library server database, remember to update the following configuration files:

   ```
   cmbicmenv.ini
   cmbicmsrvs.ini
   ```

   See Chapter 34, "Generating configuration files", on page 515 for more information about updating configuration files.

Creating or replacing a CM Oracle resource manager database

This section describes the utility programs that are used to create or replace a Content Manager Oracle resource manager database. There are two utility programs:

- A create program
- A setup and load program

The two utility programs must be executed in the correct order as outlined in the steps below.

Make sure that you have met all of the prerequisites for installing an Oracle database. For details about the prerequisites, refer to the section that applies to your operating system as follows:

For the Windows operating system
See the section "Oracle database on a Windows system" on page 86.

For the AIX operating system
See the section "Oracle database on an AIX system" on page 222.

For the Solaris operating system
See the section "Oracle database on a Solaris system" on page 335.

To start the utility program to create or replace a resource manager database:

On a Windows system

1. Open the Command Prompt window
2. Navigate to the Content Manager directory (%icmroot%\config\), for example:
   ```
   c:\Program Files\ibm\Cm81\Config\
   ```
3. Enter the following command to create the database:
   ```
   icmcreatermdb.ora
   ```
4. Follow the instructions provided by the utility program.

   Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.
5. After you create the database, enter the following command to set up and load the database you created in the previous steps:
   ```
   icmsetuprmdb.ora
   ```

On an AIX system

1. Navigate to the Content Manager directory (%icmdll%), for example:
   ```
   /usr/lpp/icm/Config/
   ```
2. Enter the command
   ```
   icmcreatermdb.ora.sh
   ```

   Requirement: This command is case-sensitive. Enter it exactly as shown (lowercase).
3. Follow the instructions provided by the utility program.

Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.

4. After you create the database, enter the following command to set up and load the database you created in the previous steps:

```
icmsetuprmdb.ora.sh
```

Requirement: This command is case-sensitive. Enter it exactly as shown (lowercase).

On a Solaris system

1. Navigate to the Content Manager directory (%icmdll%), for example:

```
/opt/IBMicm/Config/
```

2. Enter the command

```
icmcreatermdb.ora.sh
```

Requirement: This command is case-sensitive. Enter it exactly as shown (lowercase).

3. Follow the instructions provided by the utility program.

Hint: Remember to take notes and write down the key names, user IDs, and passwords that you enter during this program.

4. After you create the database, enter the following command to set up and load the database you created in the previous steps:

```
icmsetuprmdb.ora.sh
```

Requirement: This command is case-sensitive. Enter it exactly as shown (lowercase).

Deploying and configuring the resource manager with WAS Advanced Edition (AE)

To complete the resource manager installation by deploying and configuring the icmrm.war file for Was Advanced Edition (AE), follow these steps:

1. Start the WebSphere Application Server
2. Create a new application server as follows:
   a. Select **Console** ⟶ **Wizards** ⟶ **Create Application Server**.
   b. The Create Application Server wizard opens. Enter the Application Server name (for example: `icmrm`, the default name used during the installation program). Verify that the **Node to Install Server on** option contains the correct information. Click **Next**.
   c. The Enabling other Services window opens. Click **Next**.
   d. Completing the Create Application Server Wizard window opens. Click **Finish**.

e. An information dialog window appears showing that the server was created successfully. Click **OK**.

3. Select **Console ⟶ Wizards ⟶ Install Enterprise Application**
4. The Install Enterprise Application Wizard dialog window opens. Select the **Install stand-alone module (*.war, *.jar)** radio button. Complete either step **a** or step **b** to navigate to the war file (that was created during the installation program) as follows:
   a. Enter the full path for the war file in the **Path** field, for example:

      For Windows -

      `c:\Program files\IBM\CM81\Config\icmrm.war`

      For AIX -

      `/usr/lpp/icm/config/icmrm.war`

      For Solaris -

      `/opt/IBMicm/config/icmrm.war`

      Click **Open**.
   b. Or click **Browse** (next to the **Path** field) to navigate to the location of the war file. Click on the war file (for example: `icmrm.war`). Click **Open**.
   c. In the application name field, enter: `icmrm`.
   d. In the Context root for Web module field, enter: `/icmrm`.
   e. Click **Next**.
5. Click **Next** (eight more times) until the Selecting Application Servers window is displayed.

   Make sure `icmrm.war` is highlighted. (Click on the module name if it is not highlighted.)

   Click **Select Server**, and select the application server `icmrm`.

   Click **Ok**. Then, click **Next**.
6. Click **Finish** to install the application. An information dialog window appears to show that the command completed successfully.
7. Regenerate WebSphere plug-in configurations as follows:
   a. Expand the tree on the top left-hand side of the console to locate **Nodes ⟶ <hostname>**.
   b. Right-click on **<hostname>** and select **Regen Webserver Plugin**.
8. Starting the resource manager
   a. Expand the tree on the top left-hand side of the administrator’s console. Select **Nodes ⟶ <hostname> ⟶ Application Servers ⟶ icmrm**.
   b. Right-click **icmrm**.
   c. Click **Start.** A dialog appears when the resource manager is started.

Running the server configuration utility program

The server configuration utility program is provided to configure connections from a system administration client to a Content Manager library server database or to an Enterprise Information Portal system administration database.

To run the server configuration utility program:

1. Start the program:

   On a Content Manager system, click **Start → Programs → IBM Content Manager for Multiplatforms V8.2 → Server Configuration**

   On an Enterprise Information Portal system, click **Start → Programs → Enterprise Information Portal for Multiplatforms V8.2 → Server Configuration**
2. Enter the requested information about your database.

Running the library server monitor program

The library server monitor program is created automatically during the installation of the Content Manager library server component.

The library server monitor program detects the availability of resource managers to a library server database. It also:

- Counts concurrent users every 30 minutes
- Updates document routing status for Suspend and Notify flags every 10 minutes (by modifying the value in `DOCROUTINGFREQ` in `ICMSTSYSCONTROL`)
- Processes Oracle TIE updates

The library server monitor program runs as:

- A `service` on Windows (`icmplsap`)
- A `started process` on AIX (`icmxlsap`)
- A `started process` Solaris (`icmslsap`)

If the library server monitor program stops abnormally, then you need to restart it by using the following instructions:

On a Windows operating system

__ 1. Open a command window and enter:

```
icmnserv.exe
```

If you are not successful at starting this program, then you might need to register it. To register it, enter the following path in a command line window:

```
icmnserv.exe icmnlsdb "ICM LS MONITOR ICMNSLDB"
"c:\cm\icmrootd\bin\DB2\icmplsap.exe SERVIC icmnlsdb"
icmadmin password 'DB2-0'
```

Where:

`icmnlsdb/ICMNSLDB`
: Is the he name of your library server database.

`cm\icmrootd\`
: Is the location that you installed Content Manager.

`icmadmin`
: Is the library server database user ID.

`password`
: Is the library server database password.

__ 2. Go to your Service Panel

__ 3. Select the library server monitor

__ 4. Click **Start**

On an AIX or a Solaris operating system

Run the control script, which is located in the absolute path:

```
/etc/rc.cmrmproc
```

Running the First Steps program

During the installation of the CM system administration client, the First Steps program was installed on that workstation. The First Steps program is provided to do two things:

- To validate that the Content Manager components installed successfully
- To begin learning about Content Manager by working with sample data

If you want to run the First Steps program from the system administration client Windows machine, you can do so at any time:

1. Click **Start** ⟶ **Programs** ⟶ **IBM Content Manager for Multiplatforms V8.2** ⟶ **First Steps**.
2. Click **View First Steps information** to read the introduction to the First Steps process.
3. Click **Load Sample Data** to store the samples into the Content Manager database. (You can skip this step if the data is already stored)
4. Click **Work with Sample Data**. The system administration client opens. You can use it to see how Content Manager makes use of the new data model to manage objects. Some examples of what you can do are as follows:
   a. You can open the item type Policy and go to the Attributes page:

- Attributes and attribute groups appear to the left
- You can see that Policy is the name of the item type
- Insured and VIN are child components of Policy
- Address is an attribute group
- Policy_Number shows you an attribute that is free of a child component or an attribute group

b. You can explore the sample data for each object

c. You can create your own objects and add them to the sample data

d. You can delete users and re-create them

You can refer to the system administration client's online help for assistance on specific tasks.

Installing and configuring IBM License Use Management (LUM)

IBM License Use Management (LUM) is the IBM product for technical software license management. LUM tools enable software vendors and their customers to ensure that customers comply with the terms and conditions of license agreements. They check compliance through runtime monitoring of the usage of software assets.

You can decide to install LUM at any time, either before or after you install your Content Manager system. LUM consists of two products:

License Use Management Application Developer's Toolkit (LUM ADK)

LUM ADK enables software developers and vendors to implement license management in an application.

In this case, the license management (LUM ADK) is implemented within Content Manager.

The LUM runtime program must reside on the same physical workstation as the Content Manager library server. The LUM license server that tracks the licenses, may also be on the same workstation, but it is not required to be there.

All users that logon to the library server are given a unique LUM license by the license server, which monitors and tracks all LUM licenses.

License Use Management Runtime (LUM ARK)

The LUM ARK enables users of license-enabled software to manage the licensing environment. The License Use Management Runtime software is free of charge and is available for download from the IBM License Use Management Web site at http://www.ibm.com/software/lum.

The web site also includes information and news about IBM License Use Management, as well as License Use Management Runtime publications. Download the LUM Runtime documentation to help you plan and install the LUM ARK.

Installing LUM ARK for Content Manager

To install License Use Management Runtime (LUM ARK), download the code from the IBM License Use Management Web site at http://www.ibm.com/software/lum.

Install the code for your operating system, using the ″Using License Use Management Runtime″ document provided from the Web site.

Tip: License Use Management Runtime base code is part of the AIX operating system (from AIX Version 4.3.0.0 and later). To upgrade to the latest level License Use Management Runtime version, download the code from the Web site. You can learn the level of LUM runtime that is installed on your AIX machine by checking the following file:

```
/var/ifor/VERSION
```

Configuring LUM for Content Manager

Follow these steps to configure LUM:

1. Start the configuration tool for your workstation:

   For Windows, click **Start** → **Programs** → **License Use Runtime** → **Configuration Tool**

   For AIX, navigate to /usr/opt/ifor/ls/os/aix/bin

   For Solaris, navigate to /opt/lum/ls/os/solaris/bin
2. The Configuration Tool window opens. There are a number of tabs shown in the upper right portion of the window. (The **Configure As** tab is selected.)

   Unselect NodeLocked License Server (NodLS) if it is selected, then click to select the following:

   - **Network License Server**
   - **Central Registry License Server**
   - **Advanced Configuration**

   Click the blue arrow in the bottom right corner of the window to navigate to the **Direct binding** tab.
3. On the **Direct binding** tab:
   - In the **Name:** field, enter the full hostname or the ip address of the machine where the license servers will reside.
   - Select **TCP/IP**
   - Select **NetworkLS** and **Central Registry LS**

- Click the **Add** button

Click the blue arrow in the bottom right corner of the window to navigate to the **Startup** tab.

4. On the **Startup** tab, decide if you want the License Use Runtime to start automatically with the system startup.

   Click to navigate to the **User** tab.
5. On the **User** tab, accept the default, or create a new user.

   Click to navigate to the **Log** tab.
6. On the **Log** tab, select the events that you want the license server to log.

   Click to navigate to the **Direct Binding Ports** tab.
7. On the **Direct Binding Ports** tab, no modification is necessary (unless you want to change the port numbers).
8. Close the Configuration tool and **Save** the changes when prompted to do so.

Starting the license service with the Service Manager Tool

Start the service as follows:

- For Windows, click **Start** → **Programs** → **License Use Runtime** → **Service Manager Tool**. When the Service Manager Tool window opens:
  1. Click **Service** → **Start**
  2. After the services start, close the Service Manager Tool (**Service** → **Exit**).
- For AIX, navigate to:

  ```
  /usr/opt/ifor/ls/os/aix/bin/i4cfg -start
  ```
- For Solaris, navigate to:

  ```
  /opt/lum/ls/os/solaris/bin/i4cfg -start
  ```

Managing the licenses with the Basic License Tool

This section is provided to guide you to connect the License Use Runtime program with the license passwords (also known as license keys) for the Content Manager programs. To get the license keys and enroll the product, follow these steps:

1. Click **Start** → **Programs** → **License Use Runtime** → **Basic License Tool**
2. On the Basic License Tool window, click **Products** → **Enroll** → **Single Product**
3. The Enroll Product window opens. Click the **Import...** button.
4. The Import window opens. Navigate to the location where you installed Content Manager and find the **cmkey.lic** file. Select it and click the **Open** button.
5. Click **OK** to complete the enrollment of the Content Manager product.

See the ″Administering License Use Management Runtime″ section of the LUM documentation for information on how to use LUM, such as:

- Starting the basic license tool
- Performing basic administrator tasks
- Managing the licensed product
- Enrolling the product (information that is covered at the beginning of this section)
- Distributing licenses (a key part of the administration process)
- Generating reports

Uninstall procedures

See Table 168 for a list of the procedures that you can use to uninstall Content Manager or Enterprise Information Portal components.

Table 168. Uninstall procedures

Uninstall procedure
“Uninstalling Content Manager components from a Windows system”
“Uninstalling Content Manager components from an AIX system” on page 504
“Uninstalling Content Manager components from a Solaris system” on page 504
“Uninstalling Content Manager Client for Windows” on page 504
“Uninstalling Enterprise Information Portal components from a Windows system” on page 504
“Uninstalling Enterprise Information Portal components from an AIX system” on page 504
“Uninstalling Enterprise Information Portal components from a Solaris system” on page 505

Uninstalling Content Manager components from a Windows system

To uninstall Content Manager from a Windows system:

1. Click **Start** → **Settings** → **Control Panel**.
2. Double click the **Add/Remove Programs** icon.
3. Find and click **Content Manager** V8.2, then click the **Add/Remove** button.
4. Follow the directions of the Uninstall wizard to remove any or all Content Manager components from the system.
5. Make sure that all program directories have been removed from the system.
6. Reboot your workstation.

Uninstalling Content Manager components from an AIX system

To uninstall Content Manager from an AIX system:

1. Enter the following command:

   ```
   java -jar /usr/lpp/icm/uninst/uninstall.jar
   ```

2. Follow the directions of the Uninstall wizard to remove any or all Content Manager components from the system.

Uninstalling Content Manager components from a Solaris system

To uninstall Content Manager from a Solaris system:

1. Enter the following command:

   ```
   java -jar /opt/IBMicm/uninst/uninstall.jar
   ```

2. Follow the directions of the Uninstall wizard to remove any or all Content Manager components from the system.

Uninstalling Content Manager Client for Windows

To uninstall Content Manager Client for Windows:

1. Click **Start** → **Settings** → **Control Panel**.
2. Double click the **Add/Remove Programs** icon.
3. Find and click Content Manager Client for Windows, then click the **Add/Remove** button.
4. Follow the directions of the Uninstall wizard to remove any or all Content Manager components from the system.

Uninstalling Enterprise Information Portal components from a Windows system

To uninstall Enterprise Information Portal from a Windows system:

1. Click **Start** → **Settings** → **Control Panel**.
2. Double click the **Add/Remove Programs** icon.
3. Find and click **Enterprise Information Portal V8.2**, then click the **Add/Remove** button.
4. Follow the directions of the Uninstall wizard to remove any or all Enterprise Information Portal components from the system.
5. Reboot your workstation.

Uninstalling Enterprise Information Portal components from an AIX system

To uninstall Enterprise Information Portal from an AIX system:

1. Enter the following command:

   ```
   cd /usr/lpp/cmb/bin
   ./cmbxuninst.sh
   ```

2. Follow the directions of the Uninstall wizard to remove any or all Enterprise Information Portal components from the system.

Uninstalling Enterprise Information Portal components from a Solaris system

To uninstall Enterprise Information Portal from a Solaris system:

1. Enter the following command:

   ```
   cmbsuninst.sh
   ```

   When the wizard opens, select option **3**, then select option **1**.
2. Follow the directions of the Uninstall wizard to remove any or all Enterprise Information Portal components from the system.

Chapter 33. Configuring an RMI server

The procedures in this section explain how to perform these tasks on an RMI server:

- Configure the server
- Connect a client
- Configure information mining
- Configure workflow

Configuring an RMI server

To configure the RMI server:

1. Open a command prompt and change to the directory to the directory where the cmbregist81.bat (or cmbregist81.sh) file *and* the policy file are located.

   On Windows: Open cmbregist81.bat in a text editor.

   On AIX: Open /usr/lpp/cmb/bin/cmbregist81.sh in a text editor.

   On Solaris: Open /opt/IBMcmb/cmbregist81.sh in a text editor.

2. You can change the port number in the following line, or accept the default port number, 1919:

   ```
   set remotePort=1919
   ```

3. Change the following line to match your configuration:

   ```
   %JAVAHOME%\jre\bin\java -cp %CLASSPATH% -ms16M
   Djava.security.policy=.\policyDjava.rmi.server.codebase=http://com.
   ibm.mm.sdk.remote. DKRemoteMainImP%remotePort% 0 13 TS QBIC DL JDBC
   Fed V4 IP DD OD DES DB2 DJ
   ```

   0 Change 0 to a number that represents the maximum number of connections that the RMI server can concurrently process. The default is 0, which indicates that there is no maximum number of connections for this RMI server. This is the suggested setting for a single or master RMI server.

   13 Change this number to match the number of server types that follow.

   TS QBIC® DL JDBC Fed V4 IP DD OD DES DB2 DJ IC
   Server types supported by the RMI server. You can type the RMI server variables in any order, but you must type them exactly as they are listed in Table 169.

Table 169. RMI server variables

RMI server variables	When to set
DES	You are accessing Domino Extended Search servers.
DL	You are accessing Content Manager servers.
Fed	Your Enterprise Information Portal database is installed on the RMI server.
IP	You are accessing Content Manager ImagePlus for OS/390 servers.
JDBC	Your Enterprise Information Portal database is installed on the RMI server.
DD	You are accessing Domino.Doc servers.
OD	You are accessing Content Manager OnDemand servers.
QBIC	You are accessing Content Manager servers that are configured with an image search server.
TS	You are accessing Content Manager servers that are configured with a text search server.
V4	You are accessing Content Manager for AS/400 servers.
DB2	You are accessing DB2 Universal Database servers.
DJ	You are accessing DB2 DataJoiner servers.
IC	You are accessing DB2 UDB Data Warehouse Center Information Catalog Manager using the Information Catalog connector.

4. After you change the variables in the file, ensure that the number that you typed before the list of RMI server variables matches the number of server variables listed.
5. Save `cmbregist81.bat`.
6. Start the RMI server by running the `cmbregist81` command.

   On Windows:

   ```
   cmbregist81 hostname
   ```

   where *hostname* is the name of the RMI server on which you are running the command.

   On AIX:

   ```
   . /cmbregist81.sh hostname
   ```

   where *hostname* is the name of the RMI server on which you are running the command. Make sure you use the period (.) and a blank space before the command name.

7. The RMI server is now ready to use.

Configuring multiple RMI servers

You can configure Enterprise Information Portal with multiple RMI servers to distribute client requests. A group of RMI servers is called a *server pool*.

To set up an RMI server pool, you must designate one server as the master RMI server. The master server is registered with the RMI registry so that clients and other RMI servers in the server pool can connect to it. When a server pool member is registered with the master server, the master server adds the server pool member to a list.

Every client sends requests to the master server. The master server evenly delegates client requests to a member of the server pool. The server pool member fulfills the client request. The master server services a connection only when all of the server pool members have reached their maximum capacity.

For example, you start four RMI servers; one is a master server, and three are server pool members. The master server receives three client requests. The master server sends the first request to the first server, the second request to the second server, and the third request to the third server. The master server sends the fourth request to the first server, and the fifth request to the second server. If there is no limit on the number of connections, the cycle continues for as long as there are requests for servers.

Each member of the server pool and the master server must have at least one connector installed. Installing a connector from the Enterprise Information Portal Version 8.1 CD installs the RMI classes for that connection.

The difference between a master RMI server and a server pool member is how their `cmbregist81.bat` files are set.

To configure additional RMI servers to be part of a server pool:

1. Ensure that you have installed the appropriate content server connectors on the RMI server.
2. Open a command prompt and set the directory to the directory where the `cmbregist81.bat` *and* the `policy` file are located.
3. On Windows, open `cmbregist81.bat` in a text editor. On AIX and Solaris, open `cmbregist81.sh` in a text editor
4. Locate the following lines at the top of the file:

   ```
   REM Note: To point to a master RMI server do the following
   instead
   REM of the statement below
   ```

```
REM java -cp %classpath% -xms32M
Djava.rmi.server.hostname=<hostname>Djava.security.policy=.\policy
-Djava.rmi.server.codebase=http://com.ibm.mm.sdk.remote.
DKRemoteMainImp 1919 5 MasterRMIServer<MasterRMIServer host name>
1922 5 DL TS QBIC JDBC Fed
```

5. Copy and paste the following line after the `set remotePort=1919` statement:

   ```
   java -cp %classpath% -ms16MD-
   java.rmi.server.hostname=<hostname>
   -Djava.security.policy=.\policy -Djava.rmi.server.codebase=http://
   com.ibm.mm.sdk.remote.DKRemoteMainImp 1919 5
   MasterRMIServer <MasterRMIServer hostname> 1922 5
   DL TS QBIC JDBC Fed
   ```

6. In the `set remotePort` statement:

   ```
   set remotePort=1919
   ```

   Change `1919` to an available port number.

7. Delete the following line:

   ```
   %JAVAHOME%\jre\bin\java -cp %CLASSPATH% -ms16M
   -Djava.security.policy=.\policy
   -Djava.rmi.server.codebase=http://
   com.ibm.mm.sdk.remote.DKRemoteMainImp %remotePort%
   0 13 TS QBIC DL JDBC Fed V4 IP DD OD DES DB2 DJ IC ICM
   ```

8. In the line that you copied and pasted from the top of the file, change the variables to match your configuration:

   ```
   java -cp %classpath% -ms16M -
   Djava.rmi.server.hostname=<hostname>
   -Djava.security.policy=.\policy -Djava.rmi.server.codebase=http://
   com.ibm.mm.sdk.remote.DKRemoteMainImp 1919 5
   MasterRMIServer <MasterRMIServer hostname>
   1922 5 DL TS QBIC JDBC Fed
   ```

   1919 Change `1919` to the port number that the RMI server pool member is using.

   5 Change `5` to a number that represents the maximum number of connections that the RMI server can concurrently process. Note that this number automatically increases if the maximum number is reached. Type `0` to indicate there is no maximum number of connections for this RMI server pool member.

   hostname
   Change `hostname` to the host name of the RMI server pool member.

   MasterRMIServer hostname
   Change `MasterRMIServer hostname` to the host name of the RMI master server.

1922 Change 1922 to the port number that you set for the RMI master server.

5 Change this number to match the number of server types that follow.

DL TS QBIC JDBC Fed
Are the server types supported by the RMI pool member. You can type the RMI server variables in any order, but you must type them exactly as they are listed in Table 169 on page 508. The table lists the RMI variables and when to set them.

9. Save `cmbregist81.bat`.
10. Ensure that the master RMI server is running.

    Requirement: The server pool members attempt to connect to the master RMI server when they start, so you must start the master RMI server before starting the server pool members.
11. Start the RMI pool member by running the `cmbregist81` command.

    On Windows:

    ```
    cmbregist81 hostname
    ```

    where *hostname* is the host name of the RMI server where you are running the command.

    On AIX:

    ```
    . /cmbregist81.sh hostname
    ```

    where *hostname* is the host name of the RMI server where you are running the command. Make sure you use the period (.) and a blank space before the command name.

Recommendation: If you configure multiple RMI servers, you should install the federated connector on only one RMI server in the server pool.

Tip: If you have a workstation with the resource, you can run multiple RMI servers on the same workstation, but you must copy the `cmbregist81.bat` file and give the copy a different name for one of the RMI servers. For example, run one RMI server by running `cmbregist81.bat` and the second by running `cmbregist812.bat`.

Configuring the client to locate the RMI server

The `cmbclient.ini` is a file that is always installed with the administration client and every client that connects with the RMI server. If your configuration includes an RMI server, you can manually set `cmbclient.ini` on the workstation where the administration client is installed. However, at installation time, you are still prompted with the Specify RMI host name and port number window to enter the RMI host name and port number for your RMI server.

To manually set the `cmbclient.ini` file:

1. Open `cmbclient.ini` in a text editor.
2. Delete the number sign (#) next to the key words `RemoteHost` and `RemotePort`. The number sign indicates a comment in the file.
3. Type your RMI server host name and port number as follows:

   ```
   RemoteHost=ccrmi
   RemotePort=1919
   ```

   where `ccrmi` is the RMI server host name and `1919` is the RMI server port number.
4. Save `cmbclient.ini`.

Configuring workflow with an RMI server

After you install your workflow server, you can configure the workflow server as an RMI server or to connect the workflow server to the RMI server for remote administration support.

To configure the workflow server as an RMI server:

1. From a command prompt, change to the directory where the `cmbregist81.bat` *and* the `policy` file are located.
2. **On Windows:** Open `cmbsvregist81.bat` in a text editor.
3. You can change the port number in the following line, or accept the default port number, `1920`:

   ```
   set remotePort=1920
   ```
4. Change the following line to match your configuration:

   ```
   %JAVAHOME%\jre\bin\java -cp %classpath%-ms16D-
   java.security.policy=.\policy-
   Djava.rmi.server.codebase=http://com.ibm.mm.sdk.remote.
   DKRemoteServiceMainImp %remotePort% 0 1 MQWF
   ```

   0 Change `0` to a number that represents the maximum number of connections that the RMI server can concurrently process. The default is `0`, which indicates that there is no maximum number of connections for this RMI server. This is the suggested setting.

   1 Is the number of server types that are supported by the RMI server. If you use an RMI server as your workflow server, only one server type is supported: MQWF.

MQWF
Is the server type supported by the RMI server.

5. Save cmbsvregist81.bat.
6. Start the RMI server by running the cmbsvregist81.bat command.

Locating a remote administration database

If the Enterprise Information Portal administration database is located on another server, then you must set the cmbsvclient.ini file on the workflow server to connect with the remote administration database:

1. Open cmbsvclient.ini in a text editor.
2. Delete the number sign (#) next to the key words RemoteHost and RemotePort. The number sign indicates a comment in the file.
3. Type your RMI server host name and port number as follows:

   ```
   RemoteHost=yourserver
   RemotePort=yourportnumber
   ```

   where *yourserver* is the RMI server host name and *yourportnumber* is the RMI server port number.
4. Save cmbsvclient.ini.

Chapter 34. Generating configuration files

These sections describe the cmbcmenv.properties file, a list of the INI files, LDAP data source information, and the Java utilities that can conveniently create and update them.

For Enterprise Information Portal: after installing the system administration client or connectors, you can run cmbenv81.bat (Windows) or cmbenv81.sh (AIX and Solaris) to automatically set the classpath for the Java utilities.

For Content Manager: after installing the system administration client, you can run cmbicmenv81.bat (Windows) to automatically set the classpath for the Java utilities.

This section covers the following topics:

- "cmbcmenv.properties" on page 516
- "INI configuration files" on page 519
- "Lightweight Directory Access Protocol (LDAP) data sources" on page 528

cmbcmenv.properties

This properties file tells the connector where the INI files are located. It can also specify an LDAP server that can contain data source information or be used for user authentication.

Attention: Parenthesis contain comments and information, not utility parameters.

JAR files need to run utility: cmbutil81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbcmenv
```

Flags

```
Input parameter is optional if it has a default value.
-h (help)

-a <add>  (action) -c <fileSystem> (category)
  -p <directory path location for configuration files>
  -d  <directory path location cmbcmenv.properties> (default current directory)
  -seeerr  <TRUE | FALSE> (display error messages for add, update and
           delete operations (default TRUE))

-a <update>  (action) -c <fileSystem> (category)
  -p <directory path location for configuration files>
  -d  <directory path location cmbcmenv.properties> (default current directory)
  -seeerr  <TRUE | FALSE> (display error messages for add, update and
           delete operations (default TRUE))

-a <del>  (action) -c <fileSystem> (category)
  -d  <directory path location cmbcmenv.properties> (default current directory)
  -seeerr  <TRUE | FALSE> (display error messages for add, update and
           delete operations (default TRUE))

-a <add>  (action) -c <URL> (category)
  -url <URL location  for configuration files>
  -d  <directory path location cmbcmenv.properties> (default current directory)
  -seeerr  <TRUE | FALSE> (display error messages for add, update and
           delete operations (default TRUE))

-a <update>  (action) -c <URL> (category)
  -url <URL location  for configuration files>
  -d  <directory path location cmbcmenv.properties> (default current directory)
  -seeerr  <TRUE | FALSE> (display error messages for add, update and
           delete operations (default TRUE))

-a <del>  (action) -c <URL> (category)
  -d  <directory path location cmbcmenv.properties> (default current directory)
  -seeerr  <TRUE | FALSE> (display error messages for add, update and
           delete operations (default TRUE))

-a <add>  (action) -c <LDAP> (category)
  -ldapenabled <TRUE | FALSE> (LDAP enabled (default TRUE))
  -ldapdatasourcesenabled <TRUE | FALSE> (LDAP datasources enabled (default FALSE))
  -ldapuserauthenabled <TRUE | FALSE> (LDAP user authentication enabled (default FALSE))
  -ldapfactory <LDAP Java JNDI context factory> (default com.sun.jndi.ldap.LdapCtxFactory)
  -ldapstype <ACTIVE_DIRECTORY | STANDARD_LDAP> (LDAP server type (default STANDARD_LDAP))
  -ldapurl < LDAP service provider url>
  -ldapref <follow | ignore> (LDAP referral (default ignore))
  -ldapauth <simple> (LDAP referral (default simple))
  -ldapuid <LDAP principal>
  -ldapcred <LDAP credentials>
  -ldaprootdn <LDAP root domain name>
  -ldapsrchscope <SUBTREE_SCOPE | ONELEVEL_SCOPE> (LDAP search scope (default SUBTREE_SCOPE))
  -ldapprotocol <none> (LDAP protocol (default none))
  -ldapauthattr <LDAP authentication attribute> (default no value)
  -ldapport <LDAP port> (default no value)
  -ldapdescattr <LDAP user description attribute> (default DN)
  -ldapsslkeyring <LDAP IBM SSL keyring name> (default no value)
  -ldapsslpwd <LDAP IBM SSL password> (default no value)
  -ldapsslcphrs <LDAP IBM SSL ciphers> (default SSL_RSA_EXPORT_WITH_RC4_40_MD5
   SSL_RSA_EXPORT_WITH_DES40_CBC_SHA SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5)
  -d  <directory path location cmbcmenv.properties> (default current directory)
  -seeerr  <TRUE | FALSE> (display error messages for add, update and
           delete operations (default TRUE))

-a <update>  (action) -c <LDAP> (category)
  -ldapenabled <TRUE | FALSE> (LDAP enabled (default TRUE)
  -ldapdatasourcesenabled <TRUE | FALSE> (LDAP datasources enabled (default FALSE))
  -ldapuserauthenabled <TRUE | FALSE> (LDAP user authentication enabled (default FALSE))
  -ldapfactory <LDAP Java JNDI context factory> (default com.sun.jndi.ldap.LdapCtxFactory)
  -ldapstype <ACTIVE_DIRECTORY | STANDARD_LDAP> (LDAP server type (default STANDARD_LDAP))
  -ldapurl < LDAP service provider url>
  -ldapref <follow | ignore> (LDAP referral (default ignore))
  -ldapauth <simple> (LDAP referral (default simple))
  -ldapuid <LDAP principal>
  -ldapcred <LDAP credentials>
  -ldaprootdn <LDAP root domain name>
  -ldapsrchscope <SUBTREE_SCOPE | ONELEVEL_SCOPE> (LDAP search scope (default SUBTREE_SCOPE))
  -ldapprotocol <none> (LDAP protocol (default none))
  -ldapauthattr <LDAP authentication attribute> (default no value)
  -ldapport <LDAP port> (default no value)
  -ldapdescattr <LDAP user description attribute> (default DN)
  -ldapsslkeyring <LDAP IBM SSL keyring name> (default no value)
  -ldapsslpwd <LDAP IBM SSL password> (default no value)
  -ldapsslcphrs <LDAP IBM SSL ciphers> (default SSL_RSA_EXPORT_WITH_RC4_40_MD5
   SSL_RSA_EXPORT_WITH_DES40_CBC_SHA SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5)
  -d  <directory path location cmbcmenv.properties> (default current directory)
  -seeerr  <TRUE | FALSE> (display error messages for add, update and
           delete operations (default TRUE))

-a <del>  (action) -c <LDAP> (category)
  -d  <directory path location cmbcmenv.properties> (default current directory)
  -seeerr  <TRUE | FALSE> (display error messages for add, update and
           delete operations (default TRUE))
```

Examples

- This example adds the CMCFGDIR keyword and value to the cmbcmenv.properties file which points to a directory where the INI files are located.

  `java com.ibm.mm.sdk.util.cmbcmenv -a add -c fileSystem -p "c:\Program Files\IBM\CMGMT"`

- This example adds the CMCOMMON_URL keyword and value to the cmbcmenv.properties file which point to a web server directory where the INI files are located.

  `java com.ibm.mm.sdk.util.cmbcmenv -a add -c URL -url http://www.mycorp.com/cmgmt`

- This example adds the CMCOMMON_LDAP keyword and LDAP values to the cmbcmenv.properties file which point to an LDAP server where the Java Federated and/or ICM datastore data sources are to be stored. After you do this, you will need to run some other LDAP Java utilities described below to put entries for the Federated and/or ICM data sources into this LDAP server. The data sources for Federated and/or ICM datastores is only available for the Java version of these connectors.

  IBM Secure Way:

  ```
  java com.ibm.mm.sdk.util.cmbcmenv -a add -c LDAP
  ```

```
-ldapdatasourcesenabled TRUE -ldapurl ldap://www.mycorp.com
-ldapuid cn=root -ldapcred mypwd -ldaprootdn o=IBM,c=US
```

MS Active Directory:

```
java com.ibm.mm.sdk.util.cmbcmenv -a add -c LDAP
-ldapdatasourcesenabled TRUE -ldapstype ACTIVE_DIRECTORY
-ldapurl ldap://www.mycorp2.com -ldapuid myuid -ldapcred
mypwd -ldaprootdn DC=mycorp,DC=org  -ldapport 389
```

INI configuration files

These sections describe the various INI files, their purpose, cmvcmenv.properties file keywords, and the utility JAR files required to generate them. The sections also describe their Java utility usage, flags, and examples. The files listed here will be created if they do not exist. The cmbutil81.jar should always be included with the cmbutilicm81.jar, cmbutilfed81.jar and cmbutiljdbc81.jar.

For Enterprise Information Portal: after installing the system administration client or connectors, you can run cmbenv81.bat (Windows) or cmbenv81.sh (AIX and Solaris) to automatically set the classpath for the Java utilities.

For Content Manager: after installing the system administration client, you can run cmbicmenv81.bat (Windows) to automatically set the classpath for the Java utilities.

Attention: Parenthesis contain comments and information, not utility parameters. The phrase ″n/a″ means that the INI file has no utility.

Table 170. C++ INI files

INI files	Connector	cmbcmenv.properties keywords	Required utility JAR files	Page number
cmbcc2mime.ini	common	CMCFGDIR	n/a	n/a
cmbpool.ini	common	CMCFGDIR	n/a	n/a
cmbicmenv.ini	ICM	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar, cmbutilicm81.jar	Page 521
cmbicmsrvs.ini	ICM	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar, cmbutilicm81.jar	Page 522
cmbfedenv.ini	Fed	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar, cmbutilfed81.jar	Page 523
cmbds.ini	Fed	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar, cmbutilfed81.jar	Page 524
cmbdsod.ini	OD	CMCFGDIR	n/a	n/a
cmbdes.ini	DES	CMCFGDIR	n/a	n/a

Table 171. Java INI files

INI files	Connector	cmbcmenv.properties keywords	Required utility JAR files	Page number
cmbcc2mime.ini	common	CMCFGDIR, CMCOMMON_URL	n/a	n/a

Table 171. Java INI files (continued)

INI files	Connector	cmbcmenv.properties keywords	Required utility JAR files	Page number
cmbcs.ini	common	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar	Page 525
cmbclient.ini	common	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar	Page 526
cmbsvclient.ini	common	CMCFGDIR, CMCOMMON_URL	n/a	n/a
cmbsvcs.ini	common	CMCFGDIR, CMCOMMON_URL		
cmbpool.ini	common	CMCFGDIR, CMCOMMON_URL		
cmbicmenv.ini	ICM	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar, cmbutilicm81.jar	Page 521
cmbicmsrvs.ini	ICM	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar, cmbutilicm81.jar	Page 522
cmbfedenv.ini	Fed	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar, cmbutilfed81.jar	Page 523
cmbds.ini	Fed	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar, cmbutilfed81.jar	Page 524
cmbjdbcsrvs.ini	JDBC	CMCFGDIR, CMCOMMON_URL	cmbutil81.jar, cmbutiljdbc81.jar	Page 527
cmbdsod.ini	OD	CMCFGDIR, CMCOMMON_URL		
cmbdes.ini	DES	CMCFGDIR, CMCOMMON_URL		

cmbicmenv.ini (ICM connector)

This INI file has database connect information. Whenever you catalog a new database, you need to add it to this INI file.

JAR files need to run utility:

- cmbutil81.jar
- cmbutilicm81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbenvicm
```

Flags

```
Input parameter is optional if it has a default value.

 -h (help)

 -a <add>  (action)
   -s <library server database name>
   -u <database userid>
   -p <database password>
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))

 -a <update>  (action)
   -s <library server database name>
   -u <database userid>
   -p <database password>
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))

 -a <del>  (action)
   -s <library server database name>
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
```

Examples

- This example adds an entry for a library server.

  ```
  java com.ibm.mm.sdk.util.cmbenvicm -a add -s icmnlsdb -u icmconct -p
  mypwd
  ```

cmbicmsrvs.ini (ICM connector)

This INI file has datastore data source information. Whenever you catalog a new database, you need to add it to this INI file.

JAR files need to run utility:

- cmbutil81.jar
- cmbutilicm81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbsrvsicm
```

Flags

```
Input parameter is optional if it has a default value.

 -h (help)

 -a <add>  (action)
   -s <library server database name>
   -sm <database schema name>
   -r <DB2> (database representation type (default DB2))
   -sso  <TRUE | FALSE> (single signon supported (default FALSE))
   -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
   -rs  <TRUE | FALSE> (remote server indicator (default FALSE))
   -host  <hostname> (default no value)
   -port  <port number> (default no value)
   -rdb  <remote database name> (default no value)
   -node <node name> (default no value)
   -os <NT | MVS | AIX | SUN> (operating system type (default no value))

 -a <update>  (action)
   -s <library server database name>
   -sm <database schema name>
   -r <DB2> (database representation type (default DB2))
   -sso  <TRUE | FALSE> (single signon supported (default FALSE))
   -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
   -rs  <TRUE | FALSE> (remote server indicator (default FALSE))
   -host  <hostname> (default no value)
   -port  <port number> (default no value)
   -rdb  <remote database name> (default no value)
   -node <node name> (default no value)
   -os <NT | MVS | AIX | SUN> (operating system type (default no value))

 -a <del>  (action)
   -s <library server database name>
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
```

Examples

- This example adds an entry for a library server.

  ```
  java com.ibm.mm.sdk.util.cmbsrvsicm -a add -s icmnlsdb -sm ICMADMIN
  ```

cmbfedenv.ini (Federated connector)

This INI file has database connect information. Whenever you catalog a new database you need to add it to this INI file.

JAR files need to run utility:

- cmbutil81.jar
- cmbutilfed81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbenvfed
```

Flags

```
Input parameter is optional if it has a default value.

 -h (help)

 -a <add>  (action)
   -s <federated database name>
   -u <database userid>
   -p <database password>
   -d  <directory path location cmbfedenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))

 -a <update>  (action)
   -s <federated database name>
   -u <database userid>
   -p <database password>
   -d  <directory path location cmbfedenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))

 -a <del>  (action)
   -s <federated database name>
   -d  <directory path location cmbfedenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
```

Examples

- This example adds an entry for a Federated database.

  ```
  java com.ibm.mm.sdk.util.cmbenvfed -a add -s icmnlsdb -u icmconct -p mypwd
  ```

cmbds.ini (Federated connector)

This INI file has datastore data source information. Whenever you catalog a new database you need to add it to this INI file.

JAR files need to run utility:

- cmbutil81.jar
- cmbutilfed81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbdsfed
```

Flags

```
Input parameter is optional if it has a default value.

 -h (help)

 -a <add>  (action)
   -s <federated database name>
   -sm <database schema name>
   -r <DB2> (database representation type (default DB2))
   -sso  <TRUE | FALSE> (single signon supported (default FALSE))
   -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
   -rs  <TRUE | FALSE> (remote server indicator (default FALSE))
   -host  <hostname> (default no value)
   -port  <port number> (default no value)
   -rdb  <remote database name> (default no value)
   -node <node name> (default no value)
   -os <NT | MVS | AIX | SUN> (operating system type (default no value))

 -a <update>  (action)
   -s <federated database name>
   -sm <database schema name>
   -r <DB2> (database representation type (default DB2))
   -sso  <TRUE | FALSE> (single signon supported (default FALSE))
   -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
   -rs  <TRUE | FALSE> (remote server indicator (default FALSE))
   -host  <hostname> (default no value)
   -port  <port number> (default no value)
   -rdb  <remote database name> (default no value)
   -node <node name> (default no value)
   -os <NT | MVS | AIX | SUN> (operating system type (default no value))

 -a <del>  (action)
   -s <federated database name>
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
```

Examples

- This example adds an entry for a Federated database.

  ```
  java com.ibm.mm.sdk.util.cmbdsfed -a add -s icmnlsdb -sm ICMADMIN
  ```

cmbcs.ini (Java connectors)

This INI file has local or remote keywords for each datastore. Local does not use RMI. The CS package for a datastore uses the server package for that datastore internally. Remote uses RMI. The CS package for a datastore uses the client package for that datastore internally.

JAR files need to run utility: cmbutil81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbcs
```

Flags

```
Input parameter is optional if it has a default value.

 -h (help)

 -a <add>  (action)
   -dstype <datastore type>
   -local <TRUE | FALSE> (use local datastore if TRUE else use remote
          datastore if FALSE for a particular datastore type (default TRUE))
   -d  <directory path location cmbclient.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE)

 -a <update>  (action)
   -dstype <datastore type>
   -local <TRUE | FALSE> (use local datastore if TRUE else use remote
          datastore if FALSE for a particular datastore type (default TRUE))
   -d  <directory path location cmbclient.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE)

 -a <del>  (action)
   -dstype <datastore type>
   -d  <directory path location cmbclient.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE)
```

Examples

- This example adds an entry to the cmbcs.ini.

  ```
  java com.ibm.mm.sdk.util.cmbcs -a add -dstype ICM
  ```

cmbclient.ini (Java connectors)

This INI file has the datastore RMI server host name and port number.

JAR files need to run utility: cmbutil81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbclient
```

Flags

```
Input parameter is optional if it has a default value.

 -h (help)

 -a <add>  (action)
   -s <federated database name>
   -sm <database schema name>
   -r <DB2> (database representation type (default DB2))
   -sso  <TRUE | FALSE> (single signon supported (default FALSE))
   -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))

 -a <update>  (action)
   -s <federated database name>
   -sm <database schema name>
   -r <DB2> (database representation type (default DB2))
   -sso  <TRUE | FALSE> (single signon supported (default FALSE))
   -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))

 -a <del>  (action)
   -s <federated database name>
   -d  <directory path location cmbicmenv.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
```

Examples

- This example adds the entry to the cmbclient.ini.

  ```
  java com.ibm.mm.sdk.util.cmbclient -a add -hostname myhost.corp.com
  -port 1919
  ```

cmbjdbcsrvs.ini (JDBC connector)

This INI file has the datastore data sources. You need to add an entry for every JDBC server that should be returned from listDataSources in the JDBC connector.

JAR files need to run utility:

- cmbutil81.jar
- cmbutiljdbc81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbsrvsjdbc
```

Flags

```
Input parameter is optional if it has a default value.
 -h (help)

 -a <add>  (action)
   -s <JDBC datasource>
   -jdbcdriver <JDBC driver name>
   -d  <directory path location cmbjdbcsrvs.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))

 -a <update>  (action)
   -s <JDBC datasource>
   -jdbcdriver <JDBC driver name>
   -d  <directory path location cmbjdbcsrvs.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))

 -a <del>  (action)
   -s <JDBC datasource>
   -d  <directory path location cmbjdbcsrvs.ini> (default current directory)
   -seeerr  <TRUE | FALSE> (display error messages for add, update and
            delete operations (default TRUE))
```

Examples

- This example adds the entry to the cmbjdbcsrvs.ini.

  ```
  java com.ibm.mm.sdk.util.cmbsrvsjdbc -a add -s jdbc:db2:sample
  -jdbcdriver COM.ibm.db2.jdbc.app.DB2Driver
  ```

Lightweight Directory Access Protocol (LDAP) data sources

These sections describe the various LDAP data sources, their purpose, and the utility JAR files required to generate them. The sections also describe their Java utility usage, flags, and examples. The cmbutil81.jar should always be included with the cmbutilicm81.jar, cmbutilfed81.jar and cmbutiljdbc81.jar.

Attention: Parenthesis contain comments and information, not utility parameters.

Refer to Table 172 for the page number that matches your type of LDAP data source. For the ICM connector, information contained in LDAP is the same as the information contained in "cmbicmsrvs.ini (ICM connector)" on page 522. For the Federated connector, information contained in LDAP is the same as the information contained in "cmbds.ini (Federated connector)" on page 524.

Table 172. Page numbers for LDAP data sources

Java connector type	cmbcmenv.properties keywords	IBM Directory Server	Microsoft Active Directory
ICM	CMCOMMON_LDAP	Page 529	Page 532
Federated	CMCOMMON_LDAP	Page 533	Page 536

LDAP (IBM Directory Server) data sources for Java ICM connector

This utility adds entries into the LDAP server pointed to by way of the cmbcmenv.properties file.

IBM Directory Server:

1. You must create the following attributes and objects using the IBM Directory Server Directory Management Tool after your LDAP server is started. This step needs to be done before any data sources can be added.
   a. Schema → Attributes → Edit attribute
   ```
   ibm-dkdbAuth
   ibm-dkdbSchema
   ibm-dkdbType
   ibm-dkdsName
   ibm-dkdsType
   ibm-dksso
   ibm-dkscheduleAuth
   ibm-dkscheduleDayOfWeek
   ibm-dkscheduleEnable
   ibm-dkscheduleTime
   ibm-dkscheduleUID
   ibm-dkscheduleUserGroup
   ibm-dkRemote
   ibm-dkHostName
   ibm-dkPort
   ibm-dkRemoteDatabase
   ibm-dkNodeName
   ibm-dkOSType
   ```
   b. Schema → Object classes → Add object class
   ```
   ibm-dkServerType
   (with required attributes) ibm-dkdsType
   ibm-dkServerDef
   (with required attributes) ibm-dkdsName
   (with required attributes) ibm-dkdsType
   (with optional attributes) ibm-dkdbAuth
   (with optional attributes) ibm-dkdbSchema
   (with optional attributes) ibm-dkdbType
   (with optional attributes) ibm-dksso
   (with optional attributes) ibm-dkscheduleAuth
   (with optional attributes) ibm-dkscheduleDayOfWeek
   (with optional attributes) ibm-dkscheduleEnable
   (with optional attributes) ibm-dkscheduleTime
   (with optional attributes) ibm-dkscheduleUID
   (with optional attributes) ibm-dkscheduleUserGroup
   (with optional attributes) ibm-dkscheduleUID
   (with optional attributes) ibm-dkRemote
   (with optional attributes) ibm-dkHostName
   (with optional attributes) ibm-dkPort
   (with optional attributes) ibm-dkRemoteDatabase
   (with optional attributes) ibm-dkNodeName
   (with optional attributes) ibm-dkOSType
   ```

2. The LDAP administrator can have an organizational hierarchy created in LDAP if desired. The data sources can be created under this organization. You can import an LDIF file that contains the information about the organizations. This is optional.

   For example, the file below would create the SVL organization under the root o=IBM,c=US. Using the IBM Directory Server Web Administration client through your browser (ie http://myserver.corp.com/ldap), and by selecting **Database** → **Import LDIF**, the administrator can import an LDIF file.

   org.ldif

   ```
   # IBM Directory Server sample LDIF file
   #
   # The suffix "o=IBM, c=US" should be defined before attempting to load
   # this data.
   version: 1

   dn: o=IBM, c=US
   objectclass: top
   objectclass: organization
   o: IBM

   dn: ou=SVL, o=IBM, c=US
   objectclass: organizationalUnit
   ou: SVL
   ```

   When using the DKDatastoreICM.listDataSources or listDataSourceNames the connector reads the data sources from the LDAP server. In the configuration string of the datastore, you can specify the organization to use by supplying the `LDAPORG=(<org>)` (for example, org could be SVL as in the examples above). This is only valid when using the IBM Directory Server LDAP server.

JAR files need to run utility: (cmbcm81.jar, cmbicm81.jar) or icmsdk81.jar or cmbsdk81.jar

Usage

```
java com.ibm.mm.sdk.server.cmbswldapicm
```

Flags

```
Input parameter is optional if it has a default value.
 -h (help)

 -a <add>  (action)
   -c <TRUE | FALSE> (LDAP server definition context under which server
      definitions will be stored (default FALSE))
   -o <LDAP organization under which server definition context will be stored> (default no value)

 -a <del>  (action)
   -c <TRUE | FALSE> (LDAP server definition context under which server
      definitions will be stored (default FALSE))
   -o <LDAP organization under which server definition context will be stored> (default no value)
```

```
-a <add>  (action)
  -s <library server database name>
  -schema <database schema name>
  -r <DB2> (database representation type (default DB2))
  -sso  <TRUE | FALSE> (single signon supported (default FALSE))
  -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
  -o <LDAP organization under which server definition context will be stored> (default no value)
  -rs  <TRUE | FALSE> (remote server indicator (default FALSE))
  -host  <hostname> (default no value)
  -port  <port number> (default no value)
  -rdb  <remote database name> (default no value)
  -node <node name> (default no value)
  -os <NT | MVS | AIX | SUN> (operating system type (default no value))

-a <del>  (action)
  -s <library server database name>
  -o <LDAP organization under which server definition context will be stored> (default no value)
```

Examples

- This example adds the entry into LDAP:
  - Create the context if it has not already been created.

    ```
    java com.ibm.mm.sdk.server.cmbswldapicm  -a add  -c TRUE -o ou=SVL
    ```

  - Create a data source under that context if it has not already been created. (repeat)

    ```
    java com.ibm.mm.sdk.server.cmbswldapicm -a add -s icmnlsdb -r DB2
    -sso FALSE -dbauth SERVER -schema ICMADMIN -o ou=SVL
    ```

LDAP (MS Active Directory) data sources for Java ICM connector

This utility adds entries into the LDAP server pointed to by way of the cmbcmenv.properties file.

JAR files need to run utility: (cmbcm81.jar, cmbicm81.jar) or icmsdk81.jar or cmbsdk81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbadldapicm
```

Flags

```
Input parameter is optional if it has a default value.

 -h (help)

 -a <add>  (action)
   -c <TRUE | FALSE> (LDAP server definition context under which server
      definitions will be stored (default FALSE))

 -a <del>  (action)
   -c <TRUE | FALSE> (LDAP server definition context under which server
      definitions will be stored (default FALSE))

 -a <add>  (action)
   -s <library server database name>
   -schema <database schema name>
   -r <DB2> (database representation type (default DB2))
   -sso  <TRUE | FALSE> (single signon supported (default FALSE))
   -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
   -rs  <TRUE | FALSE> (remote server indicator (default FALSE))
   -host  <hostname> (default no value)
   -port  <port number> (default no value)
   -rdb  <remote database name> (default no value)
   -node <node name> (default no value)
   -os <NT | MVS | AIX | SUN> (operating system type (default no value))

 -a <del>  (action)
   -s <library server database name>
```

Examples

- This example adds the entry into LDAP:
  - Create the context if it has not already been created.

    ```
    java com.ibm.mm.sdk.server.cmbadldapicm  -a add  -c TRUE
    ```
  - Create a data source under that context if it has not already been created. (repeat)

    ```
    java com.ibm.mm.sdk.server.cmbadldapicm -a add -s icmnlsdb -r DB2
    -sso FALSE -dbauth SERVER -schema ICMADMIN
    ```

LDAP (IBM Directory Server) data sources for Java Federated connector

This utility adds entries into the LDAP server pointed to by way of the cmbcmenv.properties file.

IBM Directory Server:

1. You must create the following attributes and objects using the IBM Directory Server Directory Management Tool after your LDAP server is started. This step needs to be done before any data sources can be added.
   a. Schema → Attributes → Edit attribute

   ```
   ibm-dkdbAuth
   ibm-dkdbSchema
   ibm-dkdbType
   ibm-dkdsName
   ibm-dkdsType
   ibm-dksso
   ibm-dkscheduleAuth
   ibm-dkscheduleDayOfWeek
   ibm-dkscheduleEnable
   ibm-dkscheduleTime
   ibm-dkscheduleUID
   ibm-dkscheduleUserGroup
   ibm-dkRemote
   ibm-dkHostName
   ibm-dkPort
   ibm-dkRemoteDatabase
   ibm-dkNodeName
   ibm-dkOSType
   ```

   b. Schema → Object classes → Add object class

   ```
   ibm-dkServerType
   (with required attributes) ibm-dkdsType
   ibm-dkServerDef
   (with required attributes) ibm-dkdsName
   (with required attributes) ibm-dkdsType
   (with optional attributes) ibm-dkdbAuth
   (with optional attributes) ibm-dkdbSchema
   (with optional attributes) ibm-dkdbType
   (with optional attributes) ibm-dksso
   (with optional attributes) ibm-dkscheduleAuth
   (with optional attributes) ibm-dkscheduleDayOfWeek
   (with optional attributes) ibm-dkscheduleEnable
   (with optional attributes) ibm-dkscheduleTime
   (with optional attributes) ibm-dkscheduleUID
   (with optional attributes) ibm-dkscheduleUserGroup
   (with optional attributes) ibm-dkscheduleUID
   (with optional attributes) ibm-dkRemote
   (with optional attributes) ibm-dkHostName
   (with optional attributes) ibm-dkPort
   (with optional attributes) ibm-dkRemoteDatabase
   (with optional attributes) ibm-dkNodeName
   (with optional attributes) ibm-dkOSType
   ```

2. The LDAP administrator can have an organizational hierarchy created in LDAP if desired. The data sources can be created under this organization. You can import an LDIF file that contains the information about the organizations. This is optional.

   For example, the file below would create the SVL organization under the root o=IBM,c=US. Using the IBM Directory Server Web Administration client through your browser (ie http://myserver.corp.com/ldap), and by selecting **Database ⟶ Import LDIF**, you can import an LDIF file.

   org.ldif

   ```
   # IBM Directory Server sample LDIF file
   #
   # The suffix "o=IBM, c=US" should be defined before attempting to load
   # this data.

   version: 1

   dn: o=IBM, c=US
   objectclass: top
   objectclass: organization
   o: IBM

   dn: ou=SVL, o=IBM, c=US
   objectclass: organizationalUnit
   ou: SVL
   ```

   When using the dKDatastoreFed.listDataSources or listDataSourceNames the connector reads the data sources from the LDAP server. In the configuration string of the datastore, you can specify the organization to use by supplying the `LDAPORG=(<org>)` (for example, org could be SVL as in the examples above). This is only valid when using the IBM Directory Server LDAP server.

JAR files need to run utility: (cmbcm81.jar, cmbfed81.jar) or cmbsdk81.jar

Usage

```
java com.ibm.mm.sdk.server.cmbswldapfed
```

Flags

```
Input parameter is optional if it has a default value.

 -h (help)

 -a <add>  (action)
   -c <TRUE | FALSE> (LDAP server definition context under which server
      definitions will be stored (default FALSE))
   -o <LDAP organization under which server definition context will be stored> (default no value)

 -a <del>  (action)
   -c <TRUE | FALSE> (LDAP server definition context under which server
      definitions will be stored (default FALSE))
   -o <LDAP organization under which server definition context will be stored> (default no value)
```

```
 -a <add>  (action)
   -s <library server database name>
   -schema <database schema name>
   -r <DB2> (database representation type (default DB2))
   -sso  <TRUE | FALSE> (single signon supported (default FALSE))
   -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
   -o <LDAP organization under which server definition context will be stored> (default no value)
   -rs  <TRUE | FALSE> (remote server indicator (default FALSE))
   -host  <hostname> (default no value)
   -port  <port number> (default no value)
   -rdb  <remote database name> (default no value)
   -node <node name> (default no value)
   -os <NT | MVS | AIX | SUN> (operating system type (default no value))

 -a <del>  (action)
   -s <library server database name>
   -o <LDAP organization under which server definition context will be stored> (default no value)
```

Examples

- This example adds the entry into LDAP:
  - Create the context if it has not already been created.

    ```
    java com.ibm.mm.sdk.server.cmbswldapfed  -a add  -c TRUE -o ou=SVL
    ```
  - Create a data source under that context if it has not already been created. (repeat)

    ```
    java com.ibm.mm.sdk.server.cmbswldapfed -a add -s icmnlsdb -r DB2
    -sso FALSE -dbauth SERVER -schema ICMADMIN -o ou=SVL
    ```

LDAP (MS Active Directory) data sources for Java Federated connector

This utility adds entries into the LDAP server pointed to by way of the cmbcmenv.properties file.

JAR files need to run utility: (cmbcm81.jar, cmbfed81.jar) or cmbsdk81.jar

Usage

```
java com.ibm.mm.sdk.util.cmbadldapfed
```

Flags

```
Input parameter is optional if it has a default value.

 -h (help)

 -a <add>  (action)
   -c <TRUE | FALSE> (LDAP server definition context under which server
      definitions will be stored (default FALSE))

 -a <del>  (action)
   -c <TRUE | FALSE> (LDAP server definition context under which server
      definitions will be stored (default FALSE))

 -a <add>  (action)
   -s <library server database name>
   -schema <database schema name>
   -r <DB2> (database representation type (default DB2))
   -sso  <TRUE | FALSE> (single signon supported (default FALSE))
   -dbauth  <CLIENT | SERVER> (single signon supported (default SERVER))
   -rs  <TRUE | FALSE> (remote server indicator (default FALSE))
   -host  <hostname> (default no value)
   -port  <port number> (default no value)
   -rdb  <remote database name> (default no value)
   -node <node name> (default no value)
   -os <NT | MVS | AIX | SUN> (operating system type (default no value))

 -a <del>  (action)
   -s <library server database name>
```

Examples

- This example adds the entry into LDAP:
  - Create the context if it has not already been created.

    ```
    java com.ibm.mm.sdk.server.cmbadldapfed  -a add  -c TRUE
    ```

  - Create a data source under that context if it has not already been created. (repeat)

    ```
    java com.ibm.mm.sdk.server.cmbadldapfed -a add -s icmnlsdb -r DB2
    -sso FALSE -dbauth SERVER -schema ICMADMIN
    ```

Migrating EIP Version 7 databases

The EIP Version 8.2 migration utility converts the information stored in EIP Version7.1 databases to a format that is compatible with the new EIP Version 8.2 database. Besides the required EIP functionality, the new EIP Version 8 database contains, but does not use, all the information found in a Content Manager Version 8 database.

Planning EIP Version 7 migration

The migration process is automated and copies all the required information from the Version 7.1 database to a text file, then copies the text information into the new database.

Restriction: The EIP migration process migrates users from Version 7.1 databases. EIP Version 8.2 does not provide any automated migration of workflow data. You must redraw your Version 7.1 workflow diagrams using the EIP Version 8.2 workflow builder and redeploy the EIP Version 7.1 workflow processes.

The following list gives basic guidelines to help plan EIP Version 7.1 database migration:

- You must create and catalog one EIP Version 8.2 database for each EIP Version 7.1 database you plan to migrate.
- You can only migrate one database at a time.
- The migrated databases will require more space than the Version 7.1 database to accommodate extra rows and tables that contain unused Content Manager Version 8 database functions.
- If you plan to migrate information mining, please contact your IBM representative. Before you remove the information mining services or EIP with all features, you must backup the information mining database.

If you installed the information mining feature with EIP in an earlier release, the information mining database (information mining database) is deleted when you remove EIP. If you want to keep data in this database, back it up before you uninstall. In a db2cmd command window enter db2 list db directory. If IKF appears in the returned list of databases, the information mining database exists. In the DB2 Command Window, type db2 backup database IKF to <dir> where <dir> is a directory of your choice.

Migrating EIP 7.1 databases

This section explains how to migrate EIP 7.1 databases to EIP Version 8.2. Tip: If you are upgrading from EIP Version 8.1, no database migration is required.

The EIP Version 8.2 migration utility copies most of the EIP 7.1 data to an EIP 8.2 database. The EIP 7.1 database is preserved. Optionally, back up the EIP 7.1 databases before you migrate.

You can migrate EIP 7.1 databases two ways:

- Migrate multiple EIP 7.1 databases into one EIP 8.2 database, or
- Migrate each EIP 7.1 database into a corresponding new EIP 8.2 database

The migration utility copies the following data into the new database:

- Server definitions
- User management objects, authorization objects and user mappings
- Federated entities with federated attributes, schema mappings
- Search templates with search criteria
- User defined server type
- Mime Type, Mime to Application
- Workflow related data.

  Restriction: EIP Version 7.1 worklist information is not migrated. You must recreate the worklist information in the corresponding EIP 8.2 database.

Before you migrate

Before you use the migration utility, you must create the new database(s).

To successfully run the migration utility, install and verify the following EIP 8.2 components:

- EIP Version 8 Federated Connector (local on the system where you will perform the migration)
- EIP Version 8 administration database (federated database) (local or remote to the system where you will perform the database migration
- If you plan to migrate to or from a remote database, you must catalog the database(s) before you use the migration utility. Use DB2 Client Configuration Assistant, the DB2 command line processor, or the EIP Version 8.2 Server Configuration Utility to catalog the remote database(s).

Using the migration utility

1. Create a temporary directory on the computer where you will use the migration utility.
2. Insert the EIP Version 8 installation CD and navigate to the EIP root directory.

3. Copy `migration81.jar`, `Cmbmig7_2_8.bat` for Windows or `Cmbmig7_2_8.sh` for AIX to the temporary directory created in step 1.
4. Start the migration utility from a command prompt. For example on Windows, `C:\temp \run cmbmig_7_2_8.bat`. On AIX, the command would be `# cd /tmp/run cmbmig_7_8.sh.` **Tip**: the migration utility software automatically configures the storage space necessary for the new database(s).
5. After you start the migration utility, answer the following prompts:
   a. Name of the original database. *Example:* CMBDB1
   b. DB2 connect ID for the old database. *Example:* cmbadmin
   c. DB2 connection password. *Example:* password
   d. Schema name for the old database. *Example*: cmbadmin
   e. Name of the new database. *Example:* ICMNLSDB
   f. Library server user ID. *Example:* ICMADMIN
   g. Library server password. *Example*: password
   h. Schema name for the library server database. *Example*: ICMADMIN

      If you migrate multiple EIP 7.1 databases into one EIP 8.2 database, you must use the migration utility once for each old database and supply the same answers for steps 5-8. To migrate each EIP 7.1 database into a corresponding EIP 8.2 database, you must run the migration utility for each database with unique answers for steps 5e through 5h.

Verifying the migration

The utility displays a message when database migration completes. If errors occurred, exception messages are written to the error log file dklog.log.

To verify database migration:

1. Log on to the EIP Version 8.2 system administration client.
2. Click the drop-down list next to the Server field on the client login window.
3. Select a migrated database.
4. Type the user ID and password for the migrated database.
5. Click OK.
6. The client opens, and the name of migrated database is listed in the client main window.

Working with the EIP sample client

With the EIP sample client, Windows end users can search for and view data stored on content servers. Users can search the content servers through a direct connection. Or users can connect to the EIP federated database and select a federated search template to search multiple servers at the same time. To create the sample client, you compile Java code after installing EIP. The EIP installation program installs the sample client by default. The sample client is available in multiple languages.

To compile and access the sample client:

1. Establish the development environment: Click **Start→Programs→Enterprise Information Portal for Multiplatforms 8.2→Development Window**.
2. In a command window, change to `c:\CMBROOT\SAMPLES\java\beans\gui`
3. Select the language code for your locale from the list of files named with `CMBCA Text Resources.`*`xx`*`.java`, where *xx* is the language code for your locale. **Hint:** To help ensure an error-free compile, rename all of the CMBCA Text Resource files that do not apply to your locale, or move them to another directory.
4. Compile the sample client by typing `javac *.java`.
5. Launch the sample client by typing`java SampleClient` .
6. Select a content server, or select the federated database.
7. Type the user ID associated with the server or federated database.
8. If you log in to the federated database, you can use a federated search template to retrieve information from different content servers.
9. Select an item from the list of returned items.
10. If you searched a Content Manager OnDemand server, you must install the OnDemand Viewer to view data returned from an OnDemand server.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM
400
Advanced Peer-to-Peer Networking
AIX
AIXwindows
APPN
AS/400
C Set ++
CICS
DATABASE 2
DataJoiner
DB2
DB2 Universal Database
DisplayWrite
e-business
HotMedia
Hummingbird
ImagePlus
IMS
Micro Channel
MQSeries
MVS/ESA
NetView
OS/2
OS/390
PAL
PowerPC
PTX
QBIC
RS/6000
SecureWay
SP
VideoCharger
Visual Warehouse
VisualAge
VisualInfo
WebSphere

Approach, Domino, Lotus, Lotus 1-2-3, Lotus Notes and SmartSuite are trademarks or registered trademarks of the Lotus Development Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Glossary

This glossary defines terms and abbreviations specific to this system. Terms shown in *italics* are defined elsewhere in this glossary.

A

abstract class. An object-oriented programming *class* that represents a concept; classes derived from it represent implementations of the concept. You cannot construct an object of an abstract class; that is, it cannot be instantiated.

access control. The process of ensuring that certain functions and stored *objects* can be accessed only by authorized users in authorized ways.

access control list. A list consisting of one or more user IDs or user groups and their associated *privileges.* You use access control lists to control user access to *items* and *objects* in the Content Manager system. You use access control lists to control user access to *search templates* in the Enterprise Information Portal system.

accessory script. A *CGI script* that processes SEARCH, POST, PUT, or DELETE requests. The accessory scripts process requests that are not explicitly mapped to a CGI script named on an EXEC directive.

action list. An approved list of the actions, defined by a system administrator or some other *workflow coordinator,* that a user can perform in a *workflow* or document routing process.

address. The unique code assigned to each device or workstation connected to a network. See also *IP address.*

admission control. The process used by the server to ensure that its bandwidth needs are not compromised by new asset requests.

ADSM. See *Tivoli Storage Manager.*

aggregate bandwidth. Total throughput, in megabits per second, that moves through a server or server subsystem.

alias. In the *Internet*, a name assigned to a server that makes the server independent of the name of its host machine. The alias must be defined in the *domain name server.*

American National Standard Code for Information Interchange (ASCII). The standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters.

analog video. Video in which the information that represents images is in a continuous-scale electrical signal for amplitude and time.

API. See *application programming interface.*

application programming interface (API). A software interface that enables applications to communicate with each other. An API is the set of programming language constructs or statements that can be coded in an application program to obtain the specific functions and services provided by the underlying licensed program.

application server. Software that handles communication with the client requesting an asset and queries of the Content Manager.

archive. Persistent storage used for long-term information retention, typically very inexpensive for each stored unit and slow to access, and often in a different geographic location to protect against equipment failures and natural disasters.

ASCII. See *American National Standard Code for Information Interchange.*

asset. A digital multimedia resource that is stored for later retrieval as requested by an application. An example of such a resource is a digitized video or audio file. An asset is stored as a file in a multimedia file system supported by the *data pump*.

asset group. An organizational grouping within the multimedia file system with similar characteristics. You can use an asset group to allocate resources of a *data pump*. For example, you could establish two asset groups representing distinct departments whose assets should be kept separate for security or billing purposes.

asymmetric video compression. In multimedia applications, the use of a powerful computer to compress a video so that a less powerful system can decompress it.

asynchronous transfer mode (ATM). A transfer mode in which the information is organized into cells; it is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic. ATM is specified in international standards such as ATM Forum UNI 3.1.

attribute. A unit of data that describes a certain characteristic or property (for example, name, address, age, and so forth) of an item, and which can be used to locate that item. An attribute has a type, which indicates the range of information stored by that attribute, and a value, which is within that range. For example, information about a file in a multimedia file system, such as title, running time, or encoding type (MPEG1, H.263, and so forth). For Enterprise Information Portal, see also *federated attribute* and *native attribute.*

attribute group. Convenience grouping of one or more *attributes.* For example, Address might include the attributes Street, City, State, and Zip.

audio. The sound portion of a video signal.

Audio/Video Interleaved (AVI). A RIFF (*Resource Interchange File Format*) file specification that permits audio and video data to be interleaved in a file. The separate tracks can be accessed in alternate chunks for playback or recording while maintaining sequential access on the file device.

Audio-Video Subsystem (AVS). File format for files that can contain video and audio data, video-only data, audio-only data, or image data (a single still image). The Audio-Video Subsystem format is supported by the ActionMedia II MMPM/2 Media Control interface.

AVI. See *Audio/Video Interleaved.*

AVS. See *Audio-Video Subsystem.*

B

background. The conditions under which low priority, non-interactive programs are run.

bandwidth. (1) The difference, expressed in *Hertz*, between the highest and the lowest frequencies of a range of frequencies. (2) In *asynchronous transfer mode* (ATM), the capacity of a virtual channel, expressed in terms of peak cell rate (PCR), sustainable cell rate (SCR), and maximum burst size (MBS). (3) A measure of the capacity of a communication transport medium (such as a TV cable) to convey data.

base attributes. A set of indexes that is assigned to each *object*. All Content Manager objects have base *attributes*.

baseband. A frequency band that uses the complete bandwidth of a transmission.

batch. (1) An accumulation of data to be processed. (2) A group of records or data processing jobs brought together for processing or transmission.

binary large object (BLOB). A sequence of bytes with a size ranging from 0 bytes to 2 gigabytes. This string does not have an associated code page and character set. Image, audio, and video objects are stored in BLOBs.

bitmap. (1) A representation of an image by an array of bits. (2) A pix map with a depth of one bit plane.

BLOB. See *binary large object.*

block. A string of data elements recorded or transmitted as a unit. The elements can be characters, words, or physical records. Disk device drivers currently use a block size of 32 KB or 256 KB to write to the disk.

broadband. A frequency band divisible into several narrower bands so that different kinds of transmissions (such as voice, video, and data) can occur at the same time. See *baseband.*

bus. A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment.

C

cache. A special-purpose buffer, smaller and faster than main storage, used to hold a copy of data that can be accessed frequently. Use of a cache reduces access time, but might increase memory requirements. See also *resource manager cache* and *LAN cache.*

caching proxy server. A proxy server that can store the documents it retrieves from other servers in a local *cache*. The catching proxy server can then respond to subsequent requests for these documents without retrieving them from other servers, a process that can improve response time.

cardinality. The number of rows in a database table.

category. See *item type.*

CGI. See *Common Gateway Interface.*

CGI script. A computer program that runs on a Web server and uses the *Common Gateway Interface (CGI)* to perform tasks that are not usually done by a Web server (for example, database access and form processing). A CGI script is a CGI program that is written in a scripting language such as Perl.

child component. Optional second or lower level of a hierarchical *item type.* Each child component is directly associated with the level above it.

CIF. See *common interchange file.*

CIU. See *common interchange unit.*

class. In object-oriented design or programming, a model or template that can be instantiated to create objects with a common definition and therefore, common properties, operations, and behavior. An object is an instance of a class.

client. A computer system or process that requests a service of another computer system or process that is typically referred to as a server. Multiple clients can share access to a common server.

client application. An application written with the Content Manager APIs to customize a user interface. An application written with the object-oriented or Internet APIs to access *content servers* from Enterprise Information Portal.

Client Application for Windows. A complete object management system provided with Content Manager and written with Content Manager APIs. It supports document and folder creation, storage, and presentation, processing, and access control. You can customize it with user exit routines and partially invoke it with APIs.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

codec. A processor that can code analog audio or video information in digital form for transmission, and decode digital data back to analog form.

collection. A group of objects with a similar set of management rules.

combined search. A query that combines one or more of the following types of searches: *parametric,* text, or image.

Common Gateway Interface (CGI). A standard for the exchange of information between a Web server and programs that are external to it. The external programs can be written in any programming language that is supported by the operating system on which the Web server is running. See *CGI script.*

common interchange file (CIF). A file that contains one ImagePlus Interchange Architecture (IPIA) data stream.

common interchange unit (CIU). The independent unit of transfer for a common interchange file (CIF). It is the part of the CIF that identifies the relationship to the receiving database. A CIF can contain multiple CIUs.

component. Generic term for a *root component* or a *child component.*

compressed audio. A method of digitally encoding and decoding several seconds of voice quality audio per single videodisc frame. This increases the storage capability to several hours of audio per videodisc. Sometimes referred to as still frame audio or sound over still.

compressed video. A video resulting from the process of digitally encoding and decoding a video image or segment using a variety of computer techniques to reduce the amount of data required to represent the content accurately.

compression. The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks.

connection manager. A Content Manager component that helps maintain connections to the library server, rather than starting a new connection for each query. The connection manager has an application programming interface.

connector class. Object-oriented programming *class* that provides standard access to APIs that are native to specific *content servers.*

constructor. In programming languages, a method that has the same name as a class and is used to create and initialize objects of that class.

container. An element of the user interface that holds objects. In the *folder manager,* an *object* that can contain other folders or documents.

content class. See *MIME type.*

content server. A software system that stores multimedia and business data and the related metadata required for users to work with that data. Content Manager and Content Manager ImagePlus for OS/390 are examples of content servers.

controller. The functional component responsible for resource management (load balancing and admission control). The controller communicates with one or more *data pumps* to initiate and terminate connections to clients.

cursor. A named control structure used by an application program to point to a specific row within some ordered set of rows. The cursor is used to retrieve rows from the set.

D

data format. See *MIME type.*

data pump. The combination of the disks that hold the data and the networking hardware and software required to deliver assets to clients.

data rate. The rate at which data is transmitted or received from a device. Interactive applications tend to require a high data rate, while batch applications can usually tolerate lower data rates.

datastore. (1) Generic term for a place (such as a database system, file, or directory) where data is stored. (2) In an application program, a virtual representation of a *content server.*

data striping. Storage process in which information is split into blocks (a fixed amount of data) and the blocks are written to (or read from) a series of disks in parallel.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system.

Notes:

1. The rate is expressed in bits, characters, or blocks per second, minute, or hour.
2. Corresponding equipment should be indicated; for example, modems, intermediate equipment, or source and sink.

DCA. See *document content architecture.*

DCE. See *Distributed Computing Environment*.

DDO. See *dynamic data object.*

decode. To convert data by reversing the effect of some previous encoding.

decompression. Process of restoring compressed data to its original state, so that it can be used again.

destager. A function of the Content Manager *resource manager* that moves objects from the *staging area* to the first step in the object's *migration policy*.

device driver. Software used to manage a specific device. Other software uses the device driver as the interface to the device for reading, writing, and control functions.

device manager. In a Content Manager system, the interface between the *resource manager* and one or more physical devices.

digital. Pertaining to data in the form of digits.

digital audio. Audio tones represented by machine-readable binary numbers rather than by analog recording techniques.

digital video. Video in which the information (usually including audio) is encoded as a sequence of binary digits. The information is usually compressed. It can be stored and transported just as any other digital information. Viewing digital video involves decompressing the video data, converting it to an analog form, displaying the video on a monitor, and playing the sound through an amplifier and speakers.

digitize. To convert analog video and audio signals into digital format.

digitized image. An image derived from a scanning device or a digitizing card with a camera.

Distributed Computing Environment (DCE). The Open Software Foundation (OSF) specification (or a product derived from this specification) that assists in networking. DCE provides such functions as authentication, directory service (DS), and remote procedure call (RPC).

document. An *item* that can be stored, retrieved, and exchanged among Content Manager systems and users as a separate unit. An item with the document *semantic type* is expected to contain information that forms a document, but does not necessarily imply that it is an implementation of the Content Manager document model.

An item created from a document classified item type (a specific implementation of the Content Manager document model), must contain document parts. You can use document classified item types to create items with either the document or folder semantic type.

Document parts can include varied types of content, including for example, text, images, and spreadsheets.

document content architecture (DCA). An architecture that guarantees information integrity for a document being interchanged in an office system network. DCA provides the rule for specifying form and meaning of a document. It defines revisable form text (changeable) and final form text (unchangeable).

document root directory. The primary directory where a Web server stores accessible documents. When the server receives requests that do not point to a specific directory, it tries to serve the request from this directory.

document routing process. In Content Manager a sequence of *work steps,* and the rules governing those steps, through which a *document* or *folder* travels while it is being processed.

document type definition (DTD). The rules that specify the structure for a particular class of XML documents. The DTD defines the structure with elements, attributes, and notations, and it establishes constraints for how each element, attribute, and notation can be used within the particular class of documents. A DTD is analogous to a database schema in that the DTD completely describes the structure for a particular markup language.

domain. That part of a computer network in which the data processing resources are under common control.

domain name. In the *Internet* suite of *protocols*, a name of a host system. A domain name consists of a sequence of subnames separated by a delimiter character.

domain name server. In the *Internet* suite of *protocols*, a server that responds to queries from clients for name-to-address and address-to-name mappings as well as for other information.

dotted decimal notation. The syntactical representation of an IP address. The 4 bytes of the address are written as four decimal numbers separated by periods (dots), for example, 9.37.83.123.

DTD. See *document type definition.*

dynamic data object (DDO). In an application program, a generic representation of a stored object that is used to move that object in to, and out of, storage.

E

element. An *object* that the *list manager* allocates for an application.

encode. To convert data by using a code in such a manner that reconversion to the original form is possible.

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and transmission.

extended data object (XDO). In an application program, a generic representation of a stored complex multimedia *object* that is used to move that object in to, and out of, storage. XDOs are most often contained within *DDOs.*

Extensible Markup Language (XML). A standard metalanguage for defining markup languages that was derived from, and is a subset of, SGML. XML omits the more complex and less-used parts of SGML and makes it much easier to write applications to handle document types, author and manage structured information, and transmit and share structured information across diverse computing systems. The use of XML does not require the robust applications and processing that is necessary for SGML. XML is being developed under the auspices of the World Wide Web Consortium (W3C).

External Data Representation (XDR). A standard, developed by Sun Microsystems, Incorporated, for representing data in machine-independent format.

F

F-Coupler (frequency coupler). A physical device that merges broadband analog signals with digital data on an IBM Cabling System using shielded twisted-pair wiring. The IBM F-Coupler separates analog signals and sends them from the IBM Cabling System to the workstation. The F-Coupler allows the IBM Cabling System to accommodate simultaneous analog video with data traffic on a token-ring network.

FDDI. See *Fiber Distributed Data Interface.*

feature. The visual content information that is stored in the image search server. Also, the visual traits that image search applications use to determine matches. The four *QBIC* features are average color, histogram color, positional color, and texture.

federated attribute. An Enterprise Information Portal metadata category that is mapped to *native attributes* in one or more *content servers.* For example, the federated attribute, `policy number`, can be mapped to an *attribute,* `policy num`, in Content Manager and to an attribute, `policy ID`, in Content Manager ImagePlus for OS/390.

federated collection. A grouping of objects that results from a *federated search.*

federated datastore. Virtual representation of any number of specific *content servers,* such as Content Manager.

federated entity. An Enterprise Information Portal metadata object that is comprised of *federated attributes* and optionally associated with one or more *federated text indexes.*

federated search. A query issued from Enterprise Information Portal that simultaneously searches for data in one or more *content servers,* which can be heterogeneous.

federated text index. An Enterprise Information Portal metadata object that is mapped to one or more *native text indexes* in one or more *content servers.*

Fiber Distributed Data Interface. An American National Standards Institute (ANSI) standard for a 100-Mbps LAN using optical fiber cables.

file name extension. An addition to a file name that identifies the file type (for example, text file or program file).

file system. In AIX, the method of partitioning a hard drive for storage. See also *multimedia file system.*

file system manager. The component that manages the multimedia file system.

File Transfer Protocol (FTP). In the *Internet* suite of *protocols*, an application layer protocol that uses *Transmission Control Protocol (TCP)* and Telnet services to transfer bulk-data files between machines or hosts.

firewall. (1) In communication, a functional unit that protects and controls the connection of one network to other networks. The firewall (a) prevents unwanted or unauthorized communication traffic from entering the protected network and (b) allows only selected communication traffic to leave the protected network. (2) In equipment, a partition used to control the spread of fire.

folder. An *item* of any *item type,* regardless of classification, with the folder *semantic type.* Any item with the folder semantic type contains specific folder functionality that is provided by Content Manager, in addition to all non-resource item capabilities and any additional fuctionality available from an item type classification, such as *document* or resource item. Folders can contain any number of items of any type, including documents and subfolders. A folder is indexed by *attributes.*

folder manager. The Content Manager model for managing data as online documents and folders. You can use the folder manager APIs as the primary interface between your applications and the Content Manager content servers.

fps. Frames per second. The number of frames displayed per second.

fragment. The smallest unit of file system disk space allocation. A fragment can be 512, 1024, 2048, or 4096 bytes in size. The fragment size is defined when a file system is created.

frequency coupler. See *F-coupler.*

FTP. See *File Transfer Protocol.*

full-motion video. Video reproduction at 30 frames per second (*fps*) for *NTSC* signals or 25 fps for *PAL* signals.

G

gateway. A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures.

GB. See *gigabyte.*

gigabyte (GB). (1) For processor storage, real and virtual storage, and channel volume, 2^{30}, or 1 073 741 824 bytes. (2) For disk storage capacity and communications volume, 1 000 000 000 bytes.

H

handle. A character string that represents an object, and is used to retrieve the object.

Hertz (Hz). A unit of frequency equal to one cycle per second. In the United States, line frequency is 60 Hz or a change in voltage polarity 120 times per second; in Europe, line frequency is 50 Hz or a change in voltage polarity 100 times per second.

history log. A file that keeps a record of activities for a *workflow.*

home page. The initial Web page that is returned by a Web site when you enter the address for the Web site in a Web browser. For example, if a user specifies the address for the IBM Web site, which is http://www.ibm.com, the Web page that is returned is the IBM home page. Essentially, the home page is the entry point for accessing the contents of the Web site.

host. A computer, connected to a network, which provides an access point to that network. A host can be a client, a server, or a client and a server simultaneously.

host name. In the *Internet* suite of *protocols*, the name given to a computer. Sometimes, host name refers to the fully qualified domain name; other times, it is used to mean the most specific subname of a fully qualified domain name. For example, if mycomputer.city.company.com is the fully qualified domain name, either of the following might be considered the host name:

- mycomputer.city.company.com
- mycomputer

HTML. See *Hypertext Markup Language.*

HTTP (Hypertext Transfer Protocol). In the *Internet* suite of *protocols*, the protocol that is used to transfer and display hypertext documents

HTTPd. See *HTTP daemon.*

HTTP daemon. A multithreaded Web server that receives incoming *Hypertext Transfer Protocol (HTTP)* requests.

HTTP method. An action used by the *Hypertext Transfer Protocol (HTTP)*. HTTP methods include GET, POST, and PUT.

Hypertext Markup Language (HTML). A markup language that conforms to the SGML standard and was designed primarily to support the online display of textual and graphical information that includes hypertext links.

Hz. See *Hertz.*

I

I frame (information frame). In video compression a frame that has been compressed independently of any other frames. Also referred to as a reference frame, intra frame, or still frame.

Image Object Content Architecture (IOCA). A collection of constructs used to interchange and present images.

index. To add or edit the attribute values that identify a specific *item* or *object* so that it can be retrieved later.

index class. See *item type.*

index class subset. In earlier Content Manager, a view of an *index class* that an application uses to store, retrieve, and display folders and objects.

index class view. In earlier Content Manager, the term used in the APIs for *index class subset.*

information mining. The automated process of extracting key information from text (summarization), finding predominant themes in a collection of documents (categorization), and searching for relevant documents using powerful and flexible queries.

inline. In Content Manager, an object that is online and in a drive, but has no active *mounts.* Contrast with *mounted*.

i-node. In the AIX operating system, the internal structure that describes the individual files in the operating system; there is one i-node for each file. An i-node contains the node, type, owner, and location of a file. A table of i-nodes is stored near the beginning of a *file system*.

interactive video. Combining video and computer technology so the user's actions determine the sequence and direction the application takes.

interchange. The capability to import or export an image with its index from one Content Manager ImagePlus for OS/390 system to another ImagePlus system using a *common interchange file* or *common interchange unit.*

Internet. The worldwide collection of interconnected networks that use the Internet suite of *protocols* and permit public access.

Internet Protocol (IP). In the *Internet* suite of *protocols*, a connectionless protocol that routes data through a network or interconnected networks and acts as an intermediary between the higher protocol layers and the physical network.

intranet. A private network that integrates *Internet* standards and applications (such as Web browsers) with an organization's existing computer networking infrastructure.

IOCA. See *Image Object Content Architecture.*

IP. See *Internet Protocol.*

IP address. The unique 32-bit address that specifies the actual location of each device or workstation on the *Internet*. The address field contains two parts: the first part is the network address; the second part is the host number. For example, 9.67.97.103 is an IP address.

IP multicast. Transmission of an *Internet Protocol (IP)* datagram to a set of systems that form a single multicast group. See *multicast.*

ISO-9660. Format used for files on CD-ROM. Used with DOS.

isochronous. A communications capability that delivers a signal at a specified, bounded rate, which is desirable for continuous data such as voice and full-motion video.

item. In Content Manager, generic term for an instance of an *item type.* For example, an item might be a *folder, document,* video, or image. Generic term for the smallest unit of information that Enterprise Information Portal administers. Each item has an identifier. For example, an item might be a *folder* or a *document.*

item type. A template for defining and later locating like *items,* consisting of a *root component,* zero or more *child components,* and a classification.

item type classification. A categorization within an *item type* that further identifies the *items* of that item type. All items of the same item type have the same item type classification.

Content Manager supplies the following item type classifications: *folder, document,* object, video, image, and text; users can also define their own item type classifications.

iterator. A class or construct that you use to step through a collection of objects one at a time.

J

JavaBeans™. A platform-independent, software component technology for building reusable Java components called "beans." After they are built, these beans can be made available for use by other software engineers or can be used in Java applications. Using JavaBeans, software engineers can manipulate and assemble beans in a graphical drag-and-drop development environment.

Joint Photographic Experts Group (JPEG). (1) A group that worked to establish the standard for the compression of digitized continuous-tone images. (2) The standard for still pictures developed by this group.

JPEG. See *Joint Photographic Experts Group.*

K

Kb. See *Kilobit.*

KB. See *Kilobyte.*

Kbps. *Kilobits* per second.

key field. See *attribute.*

kilobit (Kb). (1) For processor storage, real and virtual storage, and channel volume, 210 or 1024 bits. (2) For disk storage capacity and communications volume, 1000 bits.

kilobyte (KB). (1) For processor storage, real and virtual storage, and channel volume, 210 or 1024 bytes. (2) For disk storage capacity and communications volume, 1000 bytes.

L

LAN. See *local area network.*

LAN cache. An area of temporary storage on a local *resource manager* that contains a copy of objects stored on a remote resource manager.

latency. The time interval between the instant at which an instruction control unit initiates a call for data and the instant at which the actual transfer of the data starts.

LBR. See *low bit rate.*

library client. The component of a Content Manager system that provides a low-level programming interface for the library system. The library client includes APIs that are part of the software developer's kit.

library object. See *item.*

library server. The component of a Content Manager system that stores, manages, and handles queries on *items.*

link. A directional relationship between two *items:* the source and the target. You can use a set of links to model one-to-many associations. Contrast with *reference.*

local area network (LAN). A network in which a set of devices are connected to one another for communication and that can be connected to a larger network.

low bit rate (LBR). A generic term for an interleaved H.263/G.723 stream. Low bit rate streams range from 6.4 Kbps up to 384 Kbps.

M

machine-generated data structure (MGDS). (1) An IBM structured data format protocol for passing character data among the various Content Manager ImagePlus for OS/390 programs. (2) Data extracted from an image and put into general data stream (GDS) format.

management class. The term used in the APIs for *migration policy*.

Management Information Base (MIB). A collection of objects that can be accessed by means of a network management *protocol*.

maximum transmission unit (MTU). In *LANs,* the largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the MTU for *Ethernet* is 1500 bytes.

Mb. See *megabit.*

MB. See *megabyte.*

Mbps. *Megabits* per second.

MCA. See *Micro Channel architecture.*

media archiver. A physical device that is used for storing audio and video stream data. The VideoCharger is a type of media archiver.

media server. An AIX-based component of the Content Manager system that is used for storing and accessing video files.

megabit (Mb). (1) For processor storage, real and virtual storage, and channel volume, 220 or 1 048 576 bits. (2) For disk storage capacity and communications volume, 1 000 000 bits.

megabyte (MB). (1) For processor storage, real and virtual storage, and channel volume, 220 or 1 048 576 bytes. (2) For disk storage capacity and communications volume, 1 000 000 bytes.

method. In Java design or programming, the software that implements the behavior specified by an operation. Synonymous with member function in C++.

MGDS. See *machine-generated data structure.*

MIB. See *Management Information Base.*

MIB variable. A managed object that is defined in the *Management Information Base (MIB).* The managed object is defined by a textual name and a corresponding object identifier, a syntax, an access mode, a status, and a description of the semantics of the managed object. The MIB Variable contains pertinent management information that is accessible as defined by the access mode.

Micro Channel Architecture (MCA). The rules that define how subsystems and adapters use the Micro Channel *bus* in a computer. The architecture defines the services that each subsystem can or must provide.

MIDI. See *Musical Instrument Digital Interface.*

migration. (1) The process of moving data and source from one computer system to another computer system without converting the data, such as when moving to a new operating environment. (2) Installation of a new version or release of a program to replace an earlier version or release.

migration policy. A user-defined schedule for moving *objects* from one *storage class* to the next. It describes the retention and class transition characteristics for a group of objects in a storage hierarchy.

migrator. A function of the *resource manager* that checks *migration policies* and moves objects to the next *storage class* when they are scheduled to move.

MIME type. An Internet standard for identifying the type of object being transferred across the Internet. MIME types include several variants of audio, image, and video. Each object has a MIME type.

Mixed Object Document Content Architecture (MO:DCA). An IBM architecture developed to allow the interchange of object data among applications within the interchange environment and among environments.

Mixed Object Document Content Architecture–Presentation (MO:DCA–P). A subset architecture of MO:DCA that is used as an envelope to contain documents that are sent to the Content Manager ImagePlus for OS/390 workstation for displaying or printing.

M-JPEG. See *Motion JPEG.*

MO:DCA. *Mixed Object Document Content Architecture*

MO:DCA–P. *Mixed Object Document Content Architecture—Presentation*

Motion JPEG (M-JPEG) . Used for animation.

mount. To place a data medium in a position to operate.

mounted. In Content Manager, an object that is online and in a drive, with active *mounts*. Contrast with *inline*.

Moving Pictures Expert Group (MPEG). (1) A group that is working to establish a standard for compressing and storing motion video and animation in digital form. (2) The standard under development by this group.

MPEG. See *Moving Pictures Expert Group.*

MTU. See *maximum transmission unit.*

multicast. Transmission of the same data to a selected group of destinations.

multimedia. Combining different media elements (text, graphics, audio, still image, video, animation) for display and control from a computer.

multimedia file system. A *file system* that is optimized for the storage and delivery of video and audio.

Multipurpose Internet Mail Extensions (MIME) **.** See *MIME type.*

Musical Instrument Digital Interface (MIDI). A *protocol* that allows a synthesizer to send signals to another synthesizer or to a computer, or a computer to a musical instrument, or a computer to another computer.

N

name server. See *domain name server.*

National Television Standard Committee (NTSC). (1) A committee that sets the standard for color television broadcasting and video in the United States (currently in use also in Japan). (2) The standard set by the NTSC committee.

native attribute. A characteristic of an object that is managed on a specific *content server* and that is specific to that content server. For example, the *key field* `policy num` might be a native attribute in a Content Manager content server, whereas the field `policy ID` might be a native attribute in an Content Manager OnDemand content server.

native entity. An *object* that is managed on a specific *content server* and that is comprised of *native attributes.* For example, Content Manager *index classes* are native entities comprised of Content Manager *key fields.*

native text index. An index of the text *items* that are managed on a specific *content server.* For example, a single text search index on a Content Manager content server.

network table file. A text file that contains the system-specific configuration information for each node in a Content Manager system. Each node in the system must have a network table file that identifies the node and lists the nodes that it needs to connect to.

The name of a network table is FRNOLINT.TBL.

NTSC. See *National Television Standard Committee.*

O

object. Any digital content that a user can store, retrieve and manipulate as a single unit, for example, *JPEG* images, MP3 audio, *AVI* video, and a text block from a book.

Object Linking and Embedding (OLE). A Microsoft specification for both linking and embedding applications so that they can be activated from within other applications.

object server. See *resource manager.*

object server cache. See *resource manager cache.*

OLE. See *Object Linking and Embedding.*

overlay. A collection of predefined data such as lines, shading, text, boxes, or logos, that can be merged with variable data on a page during printing.

P

package. A collection of related *classes* and interfaces that provides access protection and namespace management.

page pool. The area in the shared memory segment from which buffers are allocated for data that is read from or written to disk. Page pool size is one of the file manager startup configuration parameters.

PAL. See *Phase Alternation Line.*

parametric search. A query for *objects* that is based on the *properties* of the objects.

part. See *object.*

patron. The term used in the Content Manager APIs for *user*.

pattern-matching character. See *wildcard character.*

PCI. See *Peripheral Component Interconnect.*

peak rate. The maximum rate encountered over a given period of time.

performance group. A group of file systems sharing system resources that can affect file system performance.

Peripheral Component Interconnect (PCI). A type of *bus* architecture.

persistent identifier (PID). An identifier that uniquely identifies an *object,* regardless of where it is stored. The PID consists of both an item ID and a location.

Phase Alternation Line (PAL). The television broadcast standard for European video outside of France and the countries of the former Soviet Union.

PID. See *persistent identifier.*

pin. Keeping the program from being paged out after it is loaded into memory.

port. A system or network access point for data entry or exit. In the *Internet* suite of *protocols*, a specific logical connector between the *Transmission Control Protocol (TCP)* or the *User Datagram Protocol (UDP)* and a higher-level protocol or application.

port group. A logical name used to group one or more ports (network devices or interfaces) of the same network type that can be used to reach a given end-user destination. For example, if multiple *ATM* adapters in the IBM Content Manager VideoCharger Server complex are connected to the same ATM networks, these adapters can be configured under the same port group. The controller selects ports as necessary to balance the load.

presentation formatter. A *CGI* program that defines the forms used to select and present assets to clients.

privilege. The right to access a specific *object* in a specific way. Privileges includes rights such as creating, deleting, and selecting objects stored in the system. Privileges are assigned by the administrator.

privilege set. A collection of *privileges* for working with system components and functions. The administrator assigns privilege sets to users (user IDs) and *user groups*.

property. A characteristic of an *object* that describes the object. A property can be changed or modified. Type style is an example of a property.

protocol. The meanings of, and the sequencing rules for, requests and responses used for managing a network, transferring data, and synchronizing the states of network components.

protocol gateway. A type of *firewall* that protects computers in a business network from access by users outside that network.

proxy server. A server that receives requests intended for another server and that acts on the client's behalf (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection (for example, when the client is unable to meet the security authentication requirements of the server but should be permitted some services).

purger. A function of the *resource manager* that removes *objects* from the system.

Q

QBIC. See *query by image content.*

quality of service (Do's). For *an asynchronous transfer mode (ATM)* virtual channel or a Networking BroadBand Services (NBBS) network connection, a set of communication characteristics such as end-to-end delay, jitter, and packet loss ratio.

query by image content (QBIC). A query technology that enables searches based on visual content, called features, rather than plain text. Using QBIC, you can search for objects based on their visual characteristics, such as color and texture.

query string. A character string that specifies the properties and property values for a query. You can create the query string in an application and pass it to the query.

R

RAID. See *Redundant Array of Independent Disks*.

rank. An integer value that signifies the relevance of a given part to the results of a query. A higher rank signifies a closer match.

README file. A file that should be viewed before the program associated with it is installed or run. A README file typically contains last-minute product information, installation information, or tips for using the product.

real time. The processing of information that returns a result so rapidly that the interaction appears to be instantaneous.

Real-Time Transport Protocol (RTP). A *protocol* that provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over *multicast* or unicast network services.

rebalance. Restriping and redistributing data across the available hard disks after a disk or disks have been removed from a *file system.*

Redundant Array of Independent Disks (RAID). A collection of two or more disk drives that present the image of a single disk drive to the system. In the event of a single device failure, the data can be read or regenerated from the other disk drives in the array.

reference. Single direction, one-to-one association between a root or *child component* and another *root component.* Contrast with *link.*

release. To remove suspend criteria from an *item.* A suspended item is released when the criteria have been met, or when a user with proper authority overrides the criteria and manually releases it.

Remote Method Invocation (RMI). A set of APIs that enables distributed programming. An object in one Java Virtual Machine (JVM) can invoke methods on objects in other JVMs.

remote procedure call (RPC). (1) A facility that a *client* uses to request the execution of a procedure call from a server. This facility includes a library of procedures and an external data representation. (2) A client request to a service provider located in another node.

render. To take data that is not typically image-oriented and depict or display it as an image. In Content Manager, word-processing documents can be rendered as images for display purposes.

request. The part of a Web address that follows the *protocol* and server *host name*. For example, in the *address* http://www.server.com/rfoul/sched.htm, the request is /rfoul/sched.html.

ReSerVation Protocol (RSVP). A resource reservation setup *protocol* designed for an integrated services *Internet*. The protocol provides receiver-initiated setup of resource reservations for *multicast* and unicast data flows.

Resource Interchange File Format (RIFF) . Used for storing sound or graphics for playback on different types of computer equipment.

resource manager. The component of a Content Manager system that manages *objects.* These objects are referred to by *items* stored on the *library server.*

resource manager cache. The working storage area for the *resource manager*. Also called the *staging area.*

restriping. Redistributing and rebalancing data across all available and defined disks in a *multimedia file system*. This is typically done when a disk is removed from a file system for repair or when a new disk is added to a *file system*.

RIFF. See *Resource Interchange File Format.*

RLE. See *Run-Length Encoding.*

RMI server. A server that implements the Java *Remote Method Invocation (RMI)* distributed object model.

root component. The first or only level of a hierarchical *item type,* consisting of related system- and user-defined *attributes.*

RPC. See *remote procedure call.*

RSVP. See *ReSerVation Protocol.*

RTP. See *Real-Time Transport Protocol.*

Run-Length Encoding (RLE). A type of *compression* that is based on strings of repeated, adjacent characters or symbols, which are called "runs."

S

SCSI. See *small computer system interface.*

search criteria. In Content Manager, *attribute* values that are used to retrieve a stored *item*. In Enterprise Information Portal, specific fields that an administrator defines for a *search template* that limit or further define choices available to the *users*.

search template. A form, consisting of *search criteria* designed by an administrator, for a specific type of federated search. The administrator also identifies the *users* and *user groups* who can access each search template.

semantic type. The usage or rules for an *item.* Base, annotation, and note are semantic types supplied by Content Manager; users can also define their own semantic types.

server. A functional unit that provides services to one or more clients over a network. Examples include a file server, a print server, and a mail server.

server definition. The characteristics of a specific *content server* that uniquely identify it to Enterprise Information Portal.

server inventory. The comprehensive list of *native entities* and *native attributes* from specified *content servers.*

server type definition. The list of characteristics, as identified by the administrator, required to uniquely identify a custom server of a certain type to Enterprise Information Portal.

Simple Network Management Protocol (SNMP). In the *Internet* suite of *protocols*, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's *Management Information Base (MIB)*.

small computer system interface (SCSI). A standard hardware interface that enables a variety of peripheral devices to communicate with one another.

SMIT. See *System Management Interface Tool.*

SMS. See *system-managed storage.*

SNMP. See *Simple Network Management Protocol.*

staging. The process of moving a stored *object* from an offline or low-priority device back to an online or higher priority device, usually on demand of the system or on request of a user. When a user requests an object stored in permanent storage, a working copy is written to the *staging area*.

staging area. The working storage area for the *resource manager*. Also referred to as *resource manager cache.*

stand-alone system. A preconfigured Content Manager system that installs all of the components of a Content Manager system on a single personal computer.

sticky pool. The part of the *page pool* that is made available to cache the first block of frequently used interactive files. Sticky pool size is one of the file manager startup configuration parameters.

storage class. Identifies the type of media that an object is stored on. It is not directly associated with a physical location; however, it is directly associated with the *device manager*. Types of storage classes include:

DASD

Fixed Disk

Optical

Stream

Tape

TSM

storage group. Associates a storage system to a storage class.

storage system. A generic term for storage in the Content Manager system. See *TSM volume*, *media archiver*, and *volume.*

streamed data. Any data sent over a network connection at a specified rate. A stream can be one data type or a combination of types. Data rates, which are expressed in bits per second, vary for different types of streams and networks.

stripe group. A collection of disks that are grouped together for serving media streams. The *multimedia file system* uses stripe groups to optimize delivery of multimedia *assets*.

stripe width. The size of the block that data is split into for *striping*.

striping. Splitting data to be written into equal blocks and writing blocks simultaneously to separate disk drives. Striping maximizes performance to the disks. Reading the data back is also scheduled in parallel, with a block being read concurrently from each disk then reassembled at the host.

subclass. A *class* that is derived from another class. One or more classes might be between the class and subclass.

superclass. A *class* from which a class is derived. One or more classes might be between the class and superclass.

suspend. To remove an *object* from its *workflow* and define the suspension criteria needed to activate it. Later activating the object enables it to continue processing.

system-managed storage (SMS). The Content Manager approach to storage management. The system determines object placement, and automatically manages object backup, movement, space, and security.

System Management Interface Tool (SMIT). An interface tool of the AIX operating system for installing, maintaining, configuring, and diagnosing tasks.

T

table of contents (TOC). The list of *documents* and *folders* that are contained in a folder or *workbasket.* Search results are displayed as a folder table of contents.

Tagged Image File Format (TIFF). A file format for storing high-quality graphics.

TCP. See *Transmission Control Protocol.*

TCP/IP. See *Transmission Control Protocol/Internet Protocol.*

thin client. A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

throughput. A measure of the amount of information transmitted over a network in a given period of time. For example, a network's data transfer rate is usually measured in bits per second. Throughput is a measure of performance. It is also measured in *Kbps* or *Mbps*.

TIFF. See *Tagged Image File Format.*

Tivoli Storage Manager (TSM). A *client/server* product that provides storage management and data access services in a heterogeneous environment. It supports various communication methods, provides administrative facilities to manage the backup and storage of files, and provides facilities for scheduling backup operations.

TOC. See *table of contents.*

token ring. According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations.

token-ring network. A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

Transmission Control Protocol (TCP). A communications *protocol* used in the *Internet* and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the *Internet Protocol (IP)* as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). The suite of transport and application *protocols* that run over the Internet Protocol.

TSM. See *Tivoli Storage Manager.*

TSM volume. A logical area of storage that is managed by *Tivoli Storage Manager.*

U

UDP. See *User Datagram Protocol.*

uniform resource locator (URL). A sequence of characters that represent information resources on a computer or in a network such as the Internet. This sequence of characters includes the abbreviated name of the protocol used to access the information resource and the information used by the protocol to locate the information resource. For example, in the context of the Internet, these are abbreviated names of some protocols used to access various information resources: http, ftp, gopher, telnet, and news.

user. A person who requires the services of Content Manager. This term generally refers to users of client applications, rather than the developers of applications, who use the Content Manager APIs. In Enterprise Information Portal, anyone who is identified in the Enterprise Information Portal administration program.

User Datagram Protocol (UDP). In the *Internet* suite of *protocols*, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the *Internet Protocol (IP)* to deliver datagrams.

user exit. A point in an IBM-supplied program at which a user exit routine can be given control.

user exit routine. A user-written routine that receives control at predefined *user exits*.

user group. A group consisting of one or more defined individual *users,* identified by a single group name.

user mapping. Associating Enterprise Information Portal user IDs and passwords to corresponding user IDs and passwords in one or more content servers. User mapping enables single logon to Enterprise Information Portal and multiple *content servers*.

utility server. A Content Manager component that is used by the database utilities for scheduling purposes. You configure a utility server when you configure a *resource manager* or *library server*. There is one utility server for each resource manager and each library server.

V

video mixing. The process of dynamically inserting or combining multiple *video objects* into a single object for distribution. An example would be the mixing of commercials and broadcast programs for satellite distribution.

video object. The data file containing a program recorded for playback on a computer or television set.

video-on-demand (VOD). A service for providing consumers with movies and other programming almost immediately, per request.

video stream. The path data follows when read from the IBM Content Manager VideoCharger Server system to the display unit.

VOD. See *Video-on-demand.*

volume. A representation of an actual physical storage device or unit on which the objects in your system are stored.

W

WAIS. See *Wide Area Information Service.*

WAV. A format to store digitally recorded sound.

Web server. A server that is connected to the *Internet* and is dedicated to serving Web pages.

Wide Area Information Service (WAIS). A network information system that enables clients to search documents on the World Wide Web.

wildcard character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a wildcard character.

workbasket. A collection of *documents* or *folders* that are either in process or waiting to be processed. A workbasket definition includes the rules that govern the presentation, status, and security of its contents.

workflow. In earlier Content Manager, a sequence of *workbaskets* through which a *document* or *folder* travels while it is being processed. In Enterprise Information Portal, a sequence of *work steps,* and the rules governing those steps, through which a *work packet, document,* or *folder* travels while it is being processed.

For example, `claims approval` would describe the process that an individual insurance claim must follow for approval.

workflow coordinator. In earlier Content Manager workflow, a user who receives notification that a *work item* in the *workflow* has not been processed in some specified time. The user is selected for a specific *user group* or upon creation of the workflow.

workflow state. The status of an entire *workflow*.

work item. In earlier Content Manager workflow and Enterprise Information Portal advanced workflow, any work activity that is active within a *workflow.*

worklist. A collection of *work items, documents,* or *folders* that are assigned to a user.

work packet. In Enterprise Information Portal Version 7.1, a collection of *documents* that is routed from one location to another. Users access and work with work packets through *worklists.*

work state. The status of an individual *work item*, *document*, or *folder*.

work step. A discrete point in a *workflow* or *document routing process* through which an individual *work item, document,* or *folder* must pass.

World Wide Web (WWW). A network of servers that contain programs and files. Many of the files contain hypertext links to other documents available through the network.

WWW. See *World Wide Web.*

X

XDO. See *extended data object.*

XML. See *Extensible Markup Language.*

Index

Program Number: 5724-B19

Printed in U.S.A.

GC27-1332-01

Spine information:

IBM Content Manager for
Multiplatforms

Planning and Installing Your Content
Management System

Version 8 Release 2