Oracle® Universal Content Management

Content Server Installation Guide for Windows

10*g* Release 3 (10.1.3.5)

February 2012

ORACLE®

Content Server Installation Guide for Windows, 10g Release 3 (10.1.3.5)

Contents

3 Pre-Installation Tasks and Considerations

4 Installing a New Content Server

5 Post-Installation Tasks and Considerations

6 Updating an Existing Installation

7 Starting and Stopping Content Server

A Setting Up Your Web Server

B Setting Up Your Database

C   Content Server Components

D   Setting Up Database Search and Indexing

E   Installation Script Files

F   Disassociated Installations

G   Uninstalling Content Server

Index

Preface

The Content Server Installation Guide contains information to assist administrators responsible for installing the Content Server software and setting up a content server environment on Microsoft Windows. This guide provides introductory information, installation instructions, and configuration notes.

Audience

This document is intended for system administrators or integrators. It is not intended for end-users.

Related Documents

For more information, see the following documents in the Oracle Content Server 10*g*R3 documentation set:

- *Getting Started With Content Server*

- *Content Server Planning and Implementation Guide*

- *Using Content Server in International Environments*

- *Clustering Concepts Guide*

- *Cluster Configuration Guide for Microsoft Windows*

- *Content Server Release Notes*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

x

1

About Content Server

This section covers the following topics:

- "Product Overview" on page 1-1
- "About This Guide" on page 1-1
- "Other Useful Documents" on page 1-1

1.1 Product Overview

Content Server is the foundation for a variety of Oracle content management products. It provides a flexible, secure, centralized, web-based repository that manages all phases of the content life cycle: from creation and approval to publishing, searching, expiration, and archival or disposition. Every contributor throughout the organization can easily contribute content from native desktop applications, efficiently manage business content via rich library services, and securely access that content anywhere using a web browser.

All content, regardless of content type, is stored in the web repository or database for management, reuse and access. While stored in the repository, all types of content ranging from e-mail, discussions, documents, reports, spreadsheets and records to images, multimedia or other digital formats receive the same set of fundamental core services, including library services, security, workflow, personalization, index/search, replication, and administration.

For more information about Oracle solutions and products, visit `http://www.oracle.com`.

1.2 About This Guide

This installation guide provides all information required to install Content Server version 10gR3 on a computer running the Microsoft Windows operating system (Windows 2000 Server, Windows Server 2003, or Windows Server 2008).

The information contained in this document is subject to change as the product technology evolves and as hardware, operating systems, and third-party software are created and modified.

1.3 Other Useful Documents

In addition to this installation guide, the following documents may also be useful for setting up the Content Server software. Each document is available as a PDF file for download from the Oracle Application Server documentation Library:
http://docs.oracle.com/cd/E10316_01/ouc.htm

- **Release notes:** Before proceeding with the installation of the Content Server software, make sure that you carefully read the release notes that are provided with the Content Server software. They may contain important installation considerations that did not make it into this installation guide.

- **Using Content Server in International Environments:** This document is useful if you are planning to deploy Content Server in international, multilingual environments. It contains important considerations for installing the Content Server software on non-English operating systems and also explains how Content Server should be set up to handle multilingual content.

- **Clustering Concept Guide and Clustering Installation Guide for Windows**: These documents are useful if you are planning to deploy Content Server in clustered environments. They provide background, conceptual, and installation information about the clustered Content Server product. They also discuss recommended hardware and software for various cluster server platforms.

2

Installation Overview

This section covers the following topics:

2.1 Hardware Requirements

Content Server 10gR3 for Microsoft Windows requires an industry-standard PC with Intel, AMD, or compatible processor.

Multiple Language Considerations

When setting up hardware for installation of Content Server, it is very important to choose an appropriate server character set. For example, if an intranet needs to handle both European- and Asian-language documents, it requires a Unicode server, since a single non-Unicode character set cannot support both at the same time.

2.2 Hardware Dimensioning Guidelines

The exact hardware requirements for a computer running Content Server depend on a number of factors:

- How many **content server instances** will be running on the computer? If a computer is to run multiple content server instances, the hardware requirements are generally higher.

- Will any **conversion** or **publishing** be done on the computer running the Content Server software (for example, using PDF Converter, XML Converter, Content Publisher, or Dynamic Converter)? If that is the case, the hardware requirements are generally higher.

- Will the computer running the Content Server software be used for **production** or for **development/testing** purposes? If the computer is to run in a production environment, the hardware requirements are generally higher.

- What will the **content management load** on the computer running the Content Server software be? If higher loads are anticipated, the hardware requirements are generally higher. Also, the type of load plays a role: is there a high number of managed content items or a large number of users, or a combination of both?

The tables below provides some general hardware recommendations for various content management scenarios.

Note: All scenarios in the table assume a low to medium content management load. Higher anticipated loads require further analysis of the specific application and may demand additional hardware requirements.

For all installations the CPU processor speed should be at least 1 GHz. Disk space requirement is for Content Server software only; this does not include database space or growth space for the native and web-viewable file repositories (if located on the Content Server computer).

When a third-party full-text search/index engine is used (for example, Verity), due to the CPU load caused by indexing, two CPUs (ideally) are recommended.

CS Inst.	Conversion & Publishing	Production or Development	CPU	RAM	Disk Space
1	no	development	1 CPU	1 GB	approx. 750 MB
1	no	production	ideally 2 CPUs	2 GB	approx. 750 MB
1	yes	development	1 CPU	2 GB	approx. 750 MB
1	yes	production	ideally 2 CPUs	2 GB	approx. 750 MB

The following table applies when more than one master server and one or more proxied servers are installed.

Proxied servers that were upgraded from a Content Server release prior to 10*g*R3 (including 7.*x*) require only 10 MB of hard disk space. This is because they share the *shared* directory with their master, whereas 10*g*R3-style proxied servers have their own *shared* directory.

It is recommended that the Windows paging file is at least twice the amount of installed RAM.

CS Inst.	Conv. & Publ.	Prod. or Dev.	CPU	RAM	Disk Space
>1	no	dev.	1 CPU	at least 1 GB	approx. 750 MB for each server (master or proxied)
>1	no	prod.	1 CPU per instance (ideally 2 CPUs per instance)	at least 1 GB	approx. 750 MB for each server (master or proxied)
>1	yes	dev	ideally 2 CPUs	at least 1 GB	approx. 750 MB for each server (master or proxied)
>1	yes	prod.	ideally 2 CPUs per instance	preferably 2 GB or more	approx. 750 MB for each server (master or proxied)

2.3 Memory Usage Guidelines

This section provides a rough outline of the memory usage by Content Server.

> **Note:** The table below assumes light to medium load. Heavier loads typically put higher demands on RAM usage.

In the following table for the total RAM, less RAM will work, but performance will tend to degrade due to swapping and insufficient use of caching. Total required RAM should be 475 MB.

Component	RAM	Description and Comments
Core Win32 code	100 MB	RAM; depends on features enabled.
Core Win32 code	150 MB	Win32 system cache; varies based on many things.
Core Win32 code	100 MB	Free RAM; more is better.
Admin Server Java	15 MB	One Admin Server is recommended for each master Content Server instance. Proxied instances could leave out the 15 MB for the Admin Server Java.
Content Server core Java	100 MB	This is somewhat dependent on the number of users and what they are doing. It can be as low as 50 MB, but you should allow for 100 MB.
Content Server indexer	10 MB	

Content Server also requires a database. It is recommended that the database is located on a different computer than Content Server. The RAM usage of the database core and data may fluctuate heavily, and depends on the number of files in the system, usage, and tuning. Depending on the database used and the operating conditions, it may range anywhere from fifty megabytes to several hundreds of megabytes.

2.4 CPU Performance Guidelines

The following are rough performance estimates for a 1-GHz CPU (the numbers are all per CPU and all exclusive of other CPU activity):

- 2 small file check-ins per second (somewhat limited by database, network, and file system)

- 5 simple searches per second (can be as high as 40 per second with search cache hits)

- 30 simple dynamic page deliveries per second

- 300 small static pages per second

2.5 Software Requirements

This section covers the following topics:

- "Operating System" on page 2-4

- "Java Virtual Machine (JVM)" on page 2-5

- "Web Server" on page 2-5

- "Database" on page 2-5

> **Important:** Due to the technical nature of browsers, databases, web servers, and operating systems, Oracle cannot warrant compatibility with all versions and features of third-party products.

> **Note:** Supported software and software requirements may change. For the most current supported system configurations, see the Oracle website:
> http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html

2.5.1 Operating System

Any of the following Microsoft Windows server operating systems should be properly installed and running on the target computer for the Content Server software:

- Windows 2000 Server with Service Pack 4

- Windows Server 2003, Standard Edition, with Service Pack 1 (32-bit)

- Windows Server 2003, Enterprise Edition, with Service Pack 1 (32-bit)

- Windows Server 2003 R2, Standard Edition (32-bit)

- Windows Server 2003 R2, Enterprise Edition (32-bit)

- Windows Server 2008 R2, Enterprise Edition (64-bit)

Considerations

Please note the following important considerations:

- Make sure that your Windows environment is running at the required Service Pack level and that the latest critical patches have been applied. If this is not the case, make sure that you update Windows before proceeding with the installation of the Content Server software.

- Windows Server 2008 R2, Enterprise Edition (64-bit) is the only 64-bit version of the Windows server operating system supported. Other 64-bit versions are not supported for this Content Server release.

- For the most current installation and implementation considerations, refer to the release notes in our online documentation library: http://docs.oracle.com/cd/E10316_01/ouc.htm

- It is strongly recommended that you install the Content Server software from the distribution media that was provided to you (for example, a CD-ROM). If you downloaded an ISO image, either burn a CD or mount the ISO image to install. If you obtained a zip file, unzip this file to a temporary installation location. Make sure that you do not unzip or copy the installation files to a directory that contains any spaces (for example, *C:\CS Install*) and start the installation from there. If you do, the installation process may not complete successfully and may hang under certain circumstances.

2.5.2 Java Virtual Machine (JVM)

Content Server 10*g*R3 requires a Java Virtual Machine (JVM) 1.5 to execute server-side Java programs on the web server. For new installations, Sun JVM 1.5.0_11 can be installed automatically with the Content Server software. If you want, you may point to an existing, compatible JVM on the computer that should be used for Content Server. For Windows Server 2008, a 64-bit JVM must be downloaded and installed prior to preparing and initiating the installation.

> **Note:** A client-side Java plug-in is required to run Content Server's administration applets. For further details, refer to "Web Browsers" on page 2-6.

2.5.3 Web Server

Content Server 10*g*R3 supports the following web servers:

- Microsoft Internet Information Services (IIS) 5.0 or 6.0

- Sun Java System Web Server 6.1 (with the latest Service Pack)

- Oracle iPlanet Web Server 7.0.9

- Apache 2.0.x (2.0.42 or higher) or 2.2.x

Considerations

Please note the following important considerations:

- Depending on the selected web server, some important pre-installation considerations may apply. Refer to Chapter 3, "Pre-Installation Tasks and Considerations" for further details.

- For Apache to function properly in international environments, you may need to modify Apache's `AddDefaultCharset` configuration setting (see Chapter 3, "Pre-Installation Tasks and Considerations").

- If you are using a non-English operating system, you must make sure that you use the internationalized version of the web server software.

- For late-breaking installation and implementation considerations, refer to the release notes that are shipped with the Content Server software.

2.5.4 Database

Content Server 10*g*R3 supports the following databases:

- Microsoft SQL Server 2000 (with Service Pack 4)

- Microsoft SQL Server 2005 (including Service Packs)

- Microsoft SQL Server 2008 (must be configured manually during installation)

- Oracle Database 10*g* Release 2, Standard Edition or Enterprise Edition, with SQL*Plus and SQL*Net

- Oracle9*i* Database Release 2 (version 9.2), Standard Edition or Enterprise Edition, with SQL*Plus and SQL*Net

> **Note:** Content Server 10*g*R3 only supports Oracle9*i* Database Release 2 (version 9.2), not any earlier 9.x versions. There is a known issue with Oracle9*i* versions prior to 9.2 involving update statements with date fields that can corrupt rows of data (Oracle issue 2446039).

- Sybase Adaptive Server Enterprise (ASE) 15

- IBM DB2 8.1 or 8.2

Considerations

Please note the following important considerations:

- Depending on the selected database, some important pre-installation considerations may apply. Refer to Chapter 3, "Pre-Installation Tasks and Considerations" for further details.

- It is recommended that the database is located on a different computer than the Content Server software.

- It is generally your own responsibility to determine how many database licenses are required for your specific content management application. Please contact your database vendor for more information on licensing.

- It is recommended that you apply the latest official Service Pack or critical updates to your database.

- For late-breaking installation and implementation considerations, refer to the release notes that are shipped with the Content Server software.

2.6 Web Browsers

Standard web browsers are used to view content in the content server and perform administration tasks. This section covers the following topics:

- "General Browser Considerations" on page 2-7

- "Recommended Browsers on Windows Clients" on page 2-7

- "Recommended Browsers on UNIX Clients" on page 2-9

- "Recommended Browsers on Mac Clients" on page 2-9

> **Note:** For late-breaking browser considerations, refer to the release notes that are shipped with the Content Server software.

2.6.1 General Browser Considerations

The following considerations apply to all web browsers on all client platforms (Windows, UNIX, and Mac):

- Browsers or versions other than the ones specifically mentioned in this section may also work, but there may be some issues, which are typically associated with supported layouts and advanced interface features such as option lists based on views. For example, some browser versions may only support the Classic layout, not the Trays or Top Menus layout. These browsers typically also fail to display the options of an option list based on a view.

- A client-side Java browser plug-in is required to run Content Server's administration applets. If the Administration page provides no links to the administration applets, you need the Java browser plug-in. You can download a Java plug-in at http://www.java.com.

  Please note the following:

  - It is recommended that you do not use the Microsoft JVM and Java plug-in. The applets on the administration page of Content Server 10*g*R3 are not compatible with that JVM. If you have the Microsoft Java plug-in instead of the Sun plug-in, you will only see gray boxes when you access the administration page.

  - If you are using Internet Explorer 6.0 with the Sun JVM, you may need to click the applet image twice, depending on the Microsoft security updates that have been applied. First, you will have to click the applet image to allow interaction with the applet, and then click it a second time to actually launch the applet. After the applet launches, an authentication prompt is presented.

- If you update the Sun JVM to version 1.5, there may be intermittent problems with loading Java applets in the web browser. The applets do not load, and the following error message is displayed:

```
The Java Runtime Environment cannot be loaded from <\bin\server\jvm.dll>
```

  This affects all browsers, including Internet Explorer, Mozilla, and Firefox. If you are doing a fresh install, on a new system, you should not be affected. You can resolve this issue as follows:

  1. Go into your user profile directory and locate a directory called:

     ```
     \Documents and Setting\[user]\Application Data\Sun
     ```

  2. Delete this directory, and try again. No reboot, reinstall, or additional actions should be needed to resolve the problem.

See the support web site for any additional considerations for web browsers as they come up (especially for newly released browser versions).

2.6.2 Recommended Browsers on Windows Clients

The table below lists the web browsers that are recommended for use with Content Server 10*g*R3 for client computers running on the Microsoft Windows operating system:

Supported Web Browser	Version
Microsoft Internet Explorer	5.5 SP2, 6.0 SP2, 7.0, 8.0 (*see notes below*)
Firefox	2.0+ or 3.0+

Important Considerations

Please note the following important considerations for web browsers on Windows clients:

- See also "General Browser Considerations" on page 2-7.

- Make sure that Internet Explorer uses version 5.5 or higher of Microsoft's JScript engine. Otherwise JavaScript rendering errors (for example, 'Object Not Found') may be reported. Please note that Windows XP SP2 uses JScript engine 5.6 and Windows Vista 5.7.

- Do not use Internet Explorer 5.5 SP1 for either administrative or consumer/contributor functions. This service pack is unstable and contains a number of bugs which affect the correct functioning of Content Server:

    1. If consumers with Internet Explorer 5.5 SP1 try to save a file to disk, Internet Explorer will not save the native or web-viewable file, but rather the web filter (which is an HTML page). A workaround for this is to right-click and use the Save As option.

    2. Forced refreshes (by clicking the Refresh button in Internet Explorer or pressing F5) do not always work, which means that the screen may seem refreshed but in reality is not.

    3. Status messages are not always displayed in the status bar correctly, which means that browser actions being carried out may not be reported in the status bar.

    To find out whether you have Internet Explorer 5.5 SP1, start your browser and look under Help-About Internet Explorer. If you are running SP1, the Update Versions field will say 'SP1'.

    > **Note:** Please note that these are not Content Server related issues, but bugs in Internet Explorer 5.5 SP1 which have been confirmed by Microsoft.

- In Content Server configurations with NT Security, there is a specific situation in which the login process does not behave as you might expect. If you use Internet Explorer 6.0 to log onto Content Server and you click OK in the login dialog without entering any information, you are logged into the system as if you were not prompted. You are then logged in as the user currently logged into the computer. In all other browsers, if you click OK without entering any information for Microsoft Login, you are challenged three times and then receive an error message.

    > **Note:** Please note that this is not a Content Server related issue, but an issue with Internet Explorer 6.0.

- If you access a content server running on Windows Server 2003 using Internet Explorer 6.0 on the same computer as the content server, you will see many security prompts before you can actually access the content server. This is because of security features that are built into Windows Server 2003. To turn off these prompts, remove the Internet Explorer Enhanced Security Configuration (from the **Control Panel**, select **Add or Remove Programs** and then select **Add/Remove Windows Components**). Alternatively, you can also access the content server

using a different web browser (for example, Firefox) or using Internet Explorer 6.0 from a different computer than the content server.

- If you intend to use Verity 4.5 as the search engine, it is recommended that you do not install Internet Explorer 7.0 on the content server computer due to a compatibility issue between Verity 4.5 and Internet Explorer 7.0. This is not an issue with Verity 5.5 or 6.*x*.

2.6.3 Recommended Browsers on UNIX Clients

The table below lists the web browsers that are recommended for use with Content Server 10*g*R3 for client computers running on a UNIX operating system:

Supported Web Browser	Version
Firefox	2.0+ or 3.0+
Mozilla	1.7.12+ (Sun Solaris and Linux)

Important Considerations

See "General Browser Considerations" on page 2-7.

2.6.4 Recommended Browsers on Mac Clients

The table below lists the web browsers that are recommended for use with Content Server 10*g*R3 for client computers running on the Apple Macintosh operating system:

Supported Web Browser	Version
Firefox	2.0+ or 3.0+
Safari	3.1+

Important Considerations

Please note the following important considerations for web browsers on Mac clients:

- See also "General Browser Considerations" on page 2-7.

- There are some specific considerations for using Mac clients with Content Server. See the support web site for further details.

- For Mac OS 9 or earlier, Netscape 7.0 or higher is recommended. For Mac OS X 10.1 and higher, any of the browsers in the table above can be used.

2.7 Search Solutions

By default, Content Server 10*g*R3 uses the database for its searching and indexing capabilities. The database is set up for metadata searching only, but SQL Server and Oracle can also handle full-text searching. You will need to set this up manually after Content Server installation (see Appendix D, "Setting Up Database Search and Indexing") Also, please see "Database Search and Indexing Considerations" on page D-1 before deciding on a search solution.

Add-ons are available which allow different search solutions to be used:

- Verity

- FAST

> **Note:** If you are upgrading to Content Server version 10*g*R3 from an earlier release with Verity 4.5.1, then the Verity search engine will continue to work after the upgrade to version 10*g*R3. If you want, you can switch to database searching and indexing. Please note that Content Server 10*g*R3 does not support Verity 2.7.

2.8 E-Mail Configuration

Various Content Server features, such as workflow and subscriptions, use e-mail to notify users when files require action or are available for viewing. This section covers the following topics:

- "Supported E-Mail Servers" on page 2-10
- "Supported E-Mail Clients" on page 2-10

2.8.1 Supported E-Mail Servers

Content Server sends e-mail messages using the Simple Mail Transfer Protocol (SMTP). It is compatible with any SMTP-based mail server and most mail servers with SMTP gateways.

2.8.2 Supported E-Mail Clients

Content Server sends e-mail messages to notify users of events or pending actions. All industry-standard e-mail clients are supported. If users choose to receive HTML-formatted e-mail messages (in their user profile), they must use an e-mail client that can handle HTML formatting in e-mail.

2.9 Software Distribution Packages

The Content Server software is provided as a set of distribution packages (zip files, ISO images, or CDs), one for each supported platform. The following table lists the main Windows-related items included in the Content Server software distribution packages, along with their relative location within each package.

Content Server Software	Location
Content Server software for Microsoft Windows	**Package for Microsoft Windows**: \UCM\ContentServer\win32

Java Virtual Machine	Location
Sun Java Virtual Machine (JVM) for Windows	**Package for Microsoft Windows**: \3rdParty\win32\ jdk1.5.0_11

Documentation

The Content Server software comes with an extensive documentation set, which is installed along with the Content Server software at *[CS-Install]\weblayout\help*. You can launch the full administration online help system by starting the *index.htm* file in that directory. You can also find PDF versions of the various guides in *[CS-Install]\weblayout\help\documentation*.

For the most current Content Server documentation, visit the Oracle documentation library website: http://docs.oracle.com/cd/E10316_01/ouc.htm.

2.10 Basic Installation Procedure

This section outlines the basic installation procedure for Content Server 10*g*R3, depending on the installation scenario:

- "New Installations" on page 2-11

2.10.1 New Installations

The basic procedure for new installations of Content Server 10*g*R3 is as follows:

1. Gathering information and performing tasks before the software installation. See Chapter 3, "Pre-Installation Tasks and Considerations" for details.

2. Choosing the installation language.

3. Specifying what installation task should be performed.

4. Specifying the installation location of the content server.

5. Specifying the Java Virtual Machine (JVM).

6. Specifying the location of the native file repository ('Vault').

7. Specifying the location of the web-viewable file repository (Web Layout).

8. Specifying the authentication setup (master or proxied).

9. Specifying whether an administration server should be installed.

10. Specifying the location of the web browser executable.

11. Specifying the system locale.

12. Specifying the time zone.

13. Specifying the content server port number.

14. Specifying the administration server port number (if an administration server will be set up).

15. Specifying the security filter for incoming connection addresses.

16. Specifying the URL prefix (web server relative root).

17. Specifying and configuring basic mail settings.

18. Specifying the web server HTTP address.

19. Specifying some name for the content server instance.

20. Specifying and configuring the web server to be used with the content server.

21. Specifying and configuring the database to be used with the content server, including the JDBC and database connection settings.

22. Selecting the optional components that should be installed.

23. Setting up the Admin Server service.

24. Setting up the Content Server service.

25. Specifying whether the 8.3 naming convention should be disabled (if required).

26. Installing the software files.

27. Performing tasks after software installation (depending on the selected web server and/or database). See Chapter 5, "Post-Installation Tasks and Considerations" for details.

28. Restarting the computer.

29. Starting the content server.

30. Verifying the installation.

2.10.2 Update Installations

The basic procedure for updating existing installations to Content Server 10*g*R3 is as follows:

1. Gathering information and performing tasks before the software installation. See Chapter 3, "Pre-Installation Tasks and Considerations" for details.

2. Choosing the installation language.

3. Specifying the installation location of the content server to be updated.

4. Specifying some IIS settings (if required).

5. Selecting the optional components that should be installed.

6. Installing the software files.

7. Performing tasks after software installation (depending on the selected web server and/or database). See Chapter 5, "Post-Installation Tasks and Considerations" for details.

8. Restarting the computer.

9. Starting the content server.

10. Verifying the installation.

3

Pre-Installation Tasks and Considerations

There are a number of tasks and considerations that need to be taken into account *before* installing the Content Server software. They are related to the following:

- "Windows Operating System" on page 3-1
- "Java Virtual Machine (JVM)" on page 3-2
- "Content Server Working Environment" on page 3-2
- "Web Server" on page 3-4
- "Database" on page 3-6
- "JDBC Drivers and Settings" on page 3-13
- "Search Solutions" on page 3-13
- "Accessibility of the Content Server Interface" on page 3-15

3.1 Windows Operating System

The tasks and considerations below are related to the Microsoft Windows operating system. Make sure that you read, understand and comply with each of them before installing the Content Server software.

- Make sure that your Windows environment is running at the required Service Pack level. If not, make sure that you update it before proceeding with the installation of the Content Server software.

  Service Packs for Microsoft Windows can be downloaded from the Microsoft's Internet site (`http://www.microsoft.com`). Alternatively, you can also contact your local Microsoft representative.

- You need local administrator rights for the computer that you want to install Content Server on.

- If you are planning to install the Content Server software from a shared network location rather than locally, make sure that you assign a drive letter to that network location and then install the software using the drive letter (for example, *V:\UCM\ContentServer\win32\installer.exe*). Otherwise, the installation will fail.

- You may use Terminal Services to install Content Server.

- It is recommended that you use local drives for the native and web-viewable file repositories (the "Vault" and "Web Layout," respectively). If you do need to use shared network locations, you may point to the necessary shared resources for Content Server, Web Layout, Vault, etc. using one of two methods: by a UNC path (\\Location) or via a mapped drive letter (X:\Location). Preferably you would use

UNC paths to refer to the network locations rather than mapping them, because mapped drives are disconnected when you log out of the server. However, a solution for mapped drives is provided by the new variable BEFORE_WIN_SERVICE_START_CMD which launches a batch (.bat) or command (.cmd) file that specifies the drive mapping; this will then be done automatically before the IDC services are started. You should make sure that the content server runs as a Microsoft domain user with access privileges to the UNC locations. See the Content Server Cluster Configuration guide for more details.

■ It is recommended that you exit all running Windows programs before installing the Content Server software.

■ Prior to installing on Windows Server 2008 R2 (64-bit), you must download and install a 64-bit Java virtual machine. After installing a 64-bit JVM, you must then prepare the Content Server installation files for use on a 64-bit system by running the PreInstaller.bat file located in the GenericPreinstaller directory of the distribution media. Running the PreInstaller.bat prepares the installation files and then begins the installation process.

> **Important:** Apache (32-bit) is the only web server supported for use with Content Server on Windows Server 2008 R2 (64-bit).

3.2 Java Virtual Machine (JVM)

The tasks and considerations below are related to the Java Virtual Machine (JVM). Make sure that you read, understand and comply with each of them before installing the Content Server software.

■ By default, the Sun JVM 1.5.0_11 is used with Content Server. For new installations, this JVM version is installed automatically with the Content Server software unless you indicate you want to use a different JVM. For Windows Server 2008, a 64-bit JVM must be downloaded and installed.

■ Only the JVMs provided with the Content Server software have been tested, except for Windows Server 2008 R2 Enterprise Edition (64-bit), which used the Sun JDK version 1.6.0_25 (64-bit) for testing. If you do not want to use the default JVM for Content Server (see above), use caution. Unless you are installing on a Windows Server 2008 R2 (64-bit) system, make sure that you install a JDK 1.5 compliant Java Virtual Machine (JVM) on your Content Server system before installing the Content Server software. Non-tested JVMs may cause issues.

■ If you already have another JVM on your computer than the one required for Content Server, then this is no problem. Multiple JVMs can coexist on the same computer.

3.3 Content Server Working Environment

The tasks and considerations below are related to the Content Server working environment. Make sure that you read, understand and comply with each of them before installing the Content Server software.

■ Some of the add-ons, components, and extras mentioned in this installation guide may not be available for this Content Server release. They may become available later in the release cycle.

■ Proxied server instances for Content Server 10*g*R3 take up much more disk space than proxied server for earlier releases. This is because pre-10*g*R3 proxied servers

share the *shared* directory with their master, whereas 10*g*R3-style proxied servers have their own *shared* directory.

> **Note:** If you upgrade to Content Server 10*g*R3 from an earlier release, proxied servers will continue to share the *shared* directory with their master.

■ Identify where you want the **native file repository** (the "Vault") and the **web-viewable file repository** (the "Web Layout") to be located. You will be asked for the path name of each of these locations during the installation of the Content Server software. Make sure the locations have sufficient disk space. Also, if these directories are on a system separate from the rest of Content Server, make sure that the drives are accessible and have adequate permissions.

> **Note:** It is recommended that you use local drives for the native and web-viewable file repositories. If you do need to use shared network locations, you should preferably use UNC paths (\\Location) to refer to the network locations rather than mapping them and using drive letters (X:\Location). This is because mapped drives are disconnected when you log out of the server unless you use another piece of software to have the drives mapped as a service. Make sure that the content server runs as a Microsoft domain user with access privileges to the UNC locations.

■ Identify your company's **e-mail server address** (for example, *mail.companyname.com*). You will be asked for it during the installation of the Content Server software.

■ Identify your company's Content Server **system administrator's e-mail address** (for example, *sysadmin@companyname.com*). You will be asked for it during the installation of the Content Server software.

■ Identify your company's **HTTP address** for the content server. You will be asked for it during the installation of the Content Server software.

■ Identify the **network IP address** of the content server (for example, 61.45.14.104). Please note the localhost IP address (127.0.0.1) is not sufficient. During the installation of the Content Server software, you may need to add the content server IP address to the localhost IP address in the IP address security filter (depending on the add-ons or customizations that will be used).

■ Identify the **content server port number(s)**. You will be asked for them during the installation of the Content Server software. If you plan to use multiple content server instances on the same computer (both master and proxied), make sure that you use different port numbers for each instance.

■ Identify the **admin server port number(s)**. You will be asked for them during the installation of the Content Server software. If you plan to use multiple master content servers on the same computer, make sure that you use different port numbers for each master instance. Please note that proxied instances share the Admin server port number with their associated master instance.

■ If required, identify the **user name and password** that the content server and/or admin server should run as. You will be asked for this information during the installation of the Content Server software. If you choose not to run these services as a specific user, they will be set up to run as 'localhost'.

- Identify the **web server** that you will be using with Content Server: IIS, Sun, or .
  You will be asked for it during the installation of the Content Server software.

  For details on the exact software versions supported by Content Server , refer to
  "Software Requirements" on page 2-4.

  For pre-installation tasks and considerations specifically related to web servers,
  refer to "Web Server" on page 3-4.

- Identify the **database** that you will be using with Content Server: Microsoft SQL
  Server, Oracle, Sybase, or DB2. You will be asked for it during the installation of
  the Content Server software.

  For details on the exact software versions supported by Content Server, refer to
  "Software Requirements" on page 2-4.

  For pre-installation tasks and considerations specifically related to databases, refer
  to "Database" on page 3-6.

3.4 Web Server

A number of tasks and considerations need to be taken into account, depending on the
web server to be used in conjunction with Content Server:

- All Web Servers
- Internet Information Services (IIS)
- Sun or Oracle iPlanet Web Server
- Apache

Make sure that you read, understand and comply with each of them before installing
the Content Server software.

3.4.1 All Web Servers

The following considerations apply to all web servers that can be used in conjunction
with the Content Server software:

- The installation procedures in this document assume that you install the Content
  Server software on the same physical computer as the web server. If you want to
  distribute the content server and web server among different physical systems,
  refer to Appendix F, "Disassociated Installations."

- Make sure the web server software is installed and running correctly before
  installing the Content Server software, and record its **full path** (not required for
  IIS).

- Identify and record the **web server root**. You may be asked for it during the
  installation of the Content Server software.

> **Important:** If you plan to use Enterprise Search, make sure that you use different web roots for each content server instance (for example, Server1, Server2, etc.). Otherwise you need to make modifications to the configuration of each content server instance to provide them with a unique relative web root (HttpRelativeWebRoot value). Enterprise Search will not work if all content server instances have identical web root directory names. It is recommended that you contact support if you have already installed a content server instance and need to change its web root.

- Certain third-party products designed to enhance application security in your web server may disable functionality in Content Server. In particular, bear in mind that the content server requires lengthy CGI parameters (potentially up to 20,000 characters) and arbitrary path suffixes to the content server CGI URL path.

- Identify and record the **admin user name and password** for your web server (not required for IIS). You may be asked for it during the installation of the Content Server software. (You may need to obtain the information from the system administrator.)

- During the installation of the Content Server software, you may be asked if you want to overwrite DLLs files. If that is the case, overwrite them.

3.4.2 Internet Information Services (IIS)

Please note the following considerations for Microsoft IIS web server, in addition to the general ones specified in "All Web Servers" on page 3-4.

- Internet Information Services web server is not supported when using Content Server on a Windows Server 2008 (64-bit) operating platform.

3.4.3 Sun or Oracle iPlanet Web Server

Please note the following considerations for Sun and Oracle iPlanet web servers, in addition to the general ones specified in "All Web Servers" on page 3-4:

- Make sure that the following settings are made:
  - Set the server user to Content Server's user login.
  - Set the bind-to address to the IP address of the web server.

- If you are installing multiple master content servers on the same computer, you will need to create a separate Sun web server instance for each master content server. If you use a different port number than 80 for your web server instance, you will need to include that port number as part of the HTTP address of the web server (for example, server:81).

3.4.4 Apache

Please note the following considerations for Apache (in addition to the general ones specified in "All Web Servers" on page 3-4):

- Apache 1.*x* is not supported for use with Content Server.

- Apache (32-bit) is the only web server supported for use with Content Server on Windows Server 2008 R2 (64-bit).

- Configure Apache configuration switches.

- For Apache 2.*x* to function properly in international environments, you may need to modify Apache's AddDefaultCharset configuration setting. Some browsers (particularly, Mozilla-based ones) may not show an HTML page in the character set specified in the page. This is because Apache has a configuration entry which augments the HTTP Content-Type return header to specify the character set of every page that Apache returns, and some browsers will trust the header instead of the character set as specified in the page. This can be a particular problem for the Content Server help pages, which use UTF-8 as their standard internal character set encoding. This issue tends to show up only in non-English sites because the default character set is iso-8859-1.

  To work around this issue, use the Apache configuration entry AddDefaultCharset to make it agree with the character set as specified in the web pages. This value can be determined by looking for the value %pagecharset% in the HTML tag:

  ```
  <meta http-equiv="Content-Type" content="text/html; charset=%pagecharset%">
  ```

  If the Web site is returning pages in more than one character set, then set AddDefaultCharset to the value Off or use the Location or Directory directives to scope its usage. Please note that the content server may be using different character sets depending on the source of the content in the pages. Here is an example configuration for a Japanese content server that is using the native SJIS character set:

  ```
  <Location /idcm1>
  AddDefaultCharset shift_jis
  </Location>
  <Location /idcm1/help>
  AddDefaultCharset utf-8
  </Location>
  ```

  Note that the help pages have to be separately scoped to deliver UTF-8 encoded pages.

3.5 Database

A number of tasks and considerations need to be taken into account, depending on the database to be used in conjunction with Content Server:

- All Databases
- SQL Server
- Oracle
- Sybase
- DB2

Make sure that you read, understand and comply with each of them before installing the Content Server software.

3.5.1 All Databases

The following considerations apply to all databases that can be used in conjunction with the Content Server software:

- It is recommended that the database is on a different computer than Content Server.

- Make sure the database software is installed and running correctly before installing the Content Server software.

- Make sure that you create a database user (with password) for each database instance to be used by before installing the Content Server software.

- A JDBC driver is required for Content Server to connect and interact with the database. A default JDBC driver is provided for some databases, but you can also choose a custom JDBC driver. Make sure that the driver is JDBC 3.0 compliant. During the software installation, you may choose to use the default JDBC driver or you may specify a custom driver. See "JDBC Drivers and Settings" on page 3-13 for details on the JDBC drivers that can be used with the various databases.

- If you want the Content Server installer to set up the database automatically, make sure that you create a database for each content server instance (master and proxied) before installing the Content Server software. The Content Server installer can set up the database tables if you want, but it will not create a database inside your database space. The database(s) for must already exist before the Content Server software is installed. If the database of a content server instance does not exist, its installation will fail.

- If you choose to set up your database manually, you may do so before or after installing the Content Server software. If you are using SQL Server 2008, you must opt to skip the database configuration during installation and set up the database manaully. For detailed instructions refer to Appendix B, "Setting Up Your Database."

- Each Content Server software distribution package includes a number of directories called *UCM\ContentServer\database\[db_name]*, which contains SQL scripts for installing the database tables manually (if required). If you want to use Unicode text fields in your database tables, make sure that you use the scripts in the *unicode* subdirectory of the above location. For detailed instructions refer to Appendix B, "Setting Up Your Database."

- By default, Content Server is set up to use the database to provide searching and indexing capabilities. Depending on the database used and languages being indexed, metadata and/or full-text searching can be supported. Full-text searching requires some manual configuration steps, and the language being indexed must be supported by the database being used (see Appendix D, "Setting Up Database Search and Indexing").

  Add-ons are available which allow different search solutions to be used (for example, Verity and FAST). Separate integration documentation is available for each supported search solution.

- If the database is used for searching and indexing (the default situation) and it is set up for full-text indexing, the text of each content item is stored in the database for full-text searching. It is therefore important that you size your database accordingly. Depending on the number of indexable documents, the IdcColl1 and IdcColl2 tables may become very large.

- You may choose to set up Content Server to support non-Western-European languages (for example, Russian or Japanese). If that is the case, make sure you either use a Unicode database or the language-specific operating system and database. Also, make sure you use an encoding scheme that is compatible with all languages you want to support. For further details refer to the *Using Content Server in International Environments* guide. This document is available as a PDF file in the Content Server documentation package (*integrator\internat_environments_ 10en.pdf*).

- You need some database-related information before installing the Content Server software (see below). If the Content Server installer can set up the database for you, you will be asked for this information during the installation of the Content Server software. Otherwise, you need it during the manual database setup.

  If you are not the database administrator, you may need to work with the administrator to obtain the required information.

- Identify and record the **full installation path** to the database software.

- Identify and record the **name of the database server**:

- Identify and record the **name of the Content Server database**.

- Identify and record the **listener port number**:

- Identify and record the **user ID and password** used by Content Server to connect to the database.

3.5.2 SQL Server

Please note the following considerations for Microsoft SQL Server (in addition to the general considerations mentioned in "All Databases" on page 3-6):

- No JDBC driver for SQL Server is provided with the Content Server software. You need to obtain a JDBC driver yourself and have its files available during the software installation. You can use any JDBC 3.0 compliant driver for SQL Server that runs on the Java Runtime Environment (JRE) 1.4 and later versions. The following driver has been tested and found to work reliably with Content Server:

  – **jTDS driver**: This is an open-source JDBC driver for Microsoft SQL Server (both 2000 and 2005) which provides a complete implementation of the JDBC specification. You can download the jTDS driver from http://jtds.sourceforge.net.

  Make sure that you unzip the driver distribution file prior to installing the Content Server software. The installer cannot process driver files inside a compressed zip file.

- SQL Server 2000 does not support full-text indexing of Arabic. Content Server database full-text search capabilities are limited to those supported by the database being used. SQL Server 2005 does support full-text indexing of Arabic.

- If you are using SQL Server 2008, you must opt to skip the database configuration during installation. After skipping database configuration and completing the installation, see Appendix B, "Setting Up Your Database" for steps to manually configure SQL 2008.

- Make sure that the Content Server database is a 100 MB database with a 25 MB log (minimum).

- Set the database to grow automatically at 10% intervals.

- Make sure that the database is set up to truncate logs automatically.

- By default, Content Server uses SQL Server authentication to access the SQL Server database. If you want the Content Server installer to set up the SQL Server database automatically, you must make sure that the default authentication method for SQL Server is set correctly:

  1. Launch the SQL Server Enterprise Manager.

  2. Select the database server.

3. Right-click, and choose **Properties** from the menu.

4. Open the Security tab.

5. In the Security area, make sure that the authentication is set to 'SQL Server and Windows'. (This is not the default value.)

> **Important:** If the Content Server installer detects that SQL Server is set to Windows authentication, SQL Server login warnings will be reported, and the installation will fail since no connection with the database can be established.

> **Note:** If you want to use Windows authentication rather than SQL Server authentication, it is recommended that you set up the SQL Server database manually. See Appendix B, "Setting Up Your Database."

- Verify that the SQL server you want to use with Content Server is running and available as a service.

- The standard SQL Server database administrator ('sa' or 'dbo') does not necessarily need to be the administrator of the database.

  If you want, you can assign a different user as the owner:

  1. Use SQL Server Enterprise Manager to create the database (identified in an earlier step).

  2. Create an SQL Server login (for example, dbadmin) with a password that you will remember.

  3. On the General tab of the New Login dialog, choose the newly created database from the dropdown list as the default database for the new login.

  4. On the Database Access tab, give the new login access to the newly created database.

  5. On the same tab, check 'Public' and 'Db_Owner' in the Database Roles section.

  6. Click OK to save the new login information.

  You can also use the following script to perform steps 2 through 6 (you may need to modify the variables to suit your needs):

```
EXEC sp_addlogin 'dbadmin', 'password', 'mypassword'
GO
USE CS_DB
GO
EXEC sp_adduser 'db_admin', 'db_admin'
GO
EXEC sp_addrolemember 'db_datareader', 'db_admin'
GO
EXEC sp_addrolemember 'db_datawriter', 'db_admin'
GO
EXEC sp_addrolemember 'db_ddladmin', 'db_admin'
GO
```

3.5.3 Oracle

Please note the following considerations for Oracle databases (in addition to the general considerations mentioned in "All Databases" on page 3-6):

- Install Oracle Enterprise Server with the following:

    - SQL*Plus

    - Optional: Net9 (Oracle9*i*) or Net10 (Oracle 10*g*)

- You can use either the JDBC thin client or Oracle's OCI driver for communication with Oracle. By default, the JDBC thin client is used, but you can change this after the installation. See "Setting Up Oracle" on page B-6 for further details.

- Create temporary and default tablespaces/databasespaces. Use 300 MB for the default tablespace and 100 MB for the temporary tablespace. Also, create a database user (with password) for each instance to be used by Content Server, which uses the tablespaces that you created.

    An example of creating an Oracle database user for the tablespace is shown below. In the SQL commands shown in the example, press [Enter] after each semicolon. Make sure SQL*Plus is running. Please note that you may need to modify the path and file information to suit your specific situation.

    ```
    REM Create a new temp tablespace for the temp.
    REM Set the parameters to the defaults.
    create temporary tablespace idc_temp
     tempfile 'D:\orant\oradata\oracle9\idc_temp.dbf'
       size 100m;
    REM Create new system tablespace for the CS data.
    REM Set the parameters to the defaults.
    create tablespace idc_system
     datafile 'D:\orant\oradata\oracle9\idc_system.dbf'
       size 300m
     minimum extent 1M
     default storage ( initial     1m
                       next        1m
                       pctincrease 0);
    REM Create the Oracle user and assign tablespace
    REM and temporary tablespace from the above files.
    create USER db_admin IDENTIFIED by db_admin
      temporary tablespace idc_temp
      default tablespace idc_system
      quota unlimited on idc_system;
    ```

    In order to get full functionality for all supported components, the content server has a minimum set of privileges it requires. These privileges will grant the ability to do database full-text indexing, but they are required even if you choose not to use a full-text indexing option. To simplify the control of these privileges, it is advisable to create a role (named 'contentserver') and grant the privileges directly. As a convenience, the script file *contentserverrole.sql* in the *[CS-Install]\database\ oracle\admin* directory can be run to grant the appropriate privileges to the 'contentserver' role.

- There is no requirement for changes to the default rollback segments.

- The Content Server application can use up to 100 MB of Oracle temporary space, but typically it will be no more than 25 MB.

- Content Server commits each transaction as it occurs on insert, update or delete.

- Content Server running under UTF-8 supports Oracle 10*g* ALT 32 UTF-8 encoding.

- Although it is not required, if you have more than 500,000 documents, it is recommended that you set separate tablespaces for data and indexes. To optimize performance when a query is executed, create these tablespaces on separate physical disks, so the system can concurrently scan the index and table data. The default scripts do not assume separate tablespaces.

- You may choose to set up Content Server to support language environments other than English. If that is the case, make sure you either use a Unicode database or the language-specific Windows operating system and database. Also, make sure you take the following into account:

  - For single-byte languages (English and Western European languages), create the Oracle database using the default character set.

  - For multi-byte languages (Asian languages), create the Oracle database using the native character set or UTF-8 (for multi-language support), or use the Unicode scripts to create Unicode tables within the database.

- If you use Oracle as the database, content IDs are changed to all upper-case.

3.5.4 Sybase

Please note the following considerations for Sybase (in addition to the general considerations mentioned in "All Databases" on page 3-6):

- Create temporary and default tablespaces/databasespaces. Use 300 MB for the default tablespace and 100 MB for the temporary tablespace.

- Grant resource and connect privileges to the database user.

- The following Sybase settings are required:

  - Sybase Adaptive Server installed

  - Master Device size = 250 MB

  - System Procedures Device size = 300 MB

  - Number of Connections = 25-30 per content server node

- If you have not installed Sybase yet, make sure that you select the Interactive SQL check box when you perform the installation.

- Make sure that you set the logical page size to 16 K (the default setting is 2 K). If you do not increase the logical page size, the content server cannot store long strings in the database (for example, long URLs).

- Although it is not required, if you have more than 500,000 documents, it is recommended that you set separate tablespaces for data and indexes. To optimize performance when a query is executed, create these tablespaces on separate physical disks, so the system can concurrently scan the index and table data. The default scripts do not assume separate tablespaces.

- The maximum length of memo fields with Sybase is 255 characters. If you need longer memo fields, please contact Oracle's support organization.

- You need to update the system tables for Sybase before installing the Content Server software. This needs to be done to set up JDBC connectivity to the Sybase database. Sybase has made a script available as part of their JDBC connectivity package to achieve this. The script updates the database to support the JDBC functions that allow the JDBC interface to get database information.
  The script file is called *sql_server15.0.sql*, and it can be found in the directory

\Ucm\ContentServer\database\sybase\admin\150 in each Content Server software distribution package.

- To set up the JDBC connectivity, complete the following steps:

    1. Verify that Sybase SQLServer_*[content server]* is started. If not, perform the following tasks:

        a. From the Windows Start menu, select **Settings**, **Control Panel**, **Administrative Tools**, and then **Services**.

        b. Scroll to 'Sybase SQL Server', then click **Start**.

        c. Close the Services screen.

    2. From the Windows Start menu, select **Programs**, **Sybase**, **SQL Advantage**.

        Interactive SQL is started.

    3. Use **File**, **Open** in Interactive SQL to navigate to the *\database\sybase\ admin\150* directory in the software distribution package.

    4. Double-click the file *sql_server15.0.sql*.

        The *sql_server15.0.sql* on server screen is displayed.

    5. From the menu bar, select **Query** and then select **Execute Query**.

        The Connect screen is displayed.

    6. Enter the Sybase user name and password, and then click **Connect**. The result 1 from the *sql_ server15.0.sql* screen is displayed.

    7. In the SQL Statements pane enter the following commands:

        ```
        USE Master
        go
        exec sp_dboption '<database_name>' , 'select into/bulkcopy/pllsort' , true
        go
        USE database_name
        go
        checkpoint
        go
        ```

        This statement enables privileges for altering tables.

    8. Select **Execute SQL Statement**.

    9. Close Interactive SQL. If a message window is displayed asking whether the changes should be saved, click **No**.

- Configure the Sybase database to use Data Rows as the locking scheme. (Refer to the Sybase documentation for more information.) The default locking scheme (All Pages) can be changed to Data Rows by running the following script in the Content Server software distribution package:

    ```
    \ContentServer\database\sybase\admin\rowlocking.sql
    ```

    All tables created will now use Data Rows as their locking scheme instead of All Pages. This change is necessary to avoid deadlock situations under heavy load.

3.5.5 DB2

Please note the following considerations for DB2 (in addition to the general considerations mentioned in "All Databases" on page 3-6):

- There are no redistributable JDBC drivers for DB2, and that is why you need to specify one manually for this database during the Content Server software installation. You will typically use the following two Universal JDBC driver files for DB2:

  - [*DB2_Dir*]/sqllib/java/db2jcc.jar

  - [*DB2_Dir*]/sqllib/java/db2jcc_license_XX.jar, where 'XX' is a two-letter code for the platform (typically 'CU' for Windows)]

  Copy the .jar files to a directory on the machine on which the content server is being installed. When prompted for the JDBC driver path during the installation, provide the path to the license files (for example, *c:\temp\db2cc.jar;c:\temp\ db2cc_licenseCU.jar*), ensuring each file is separated by a semicolon.

- Full-text searching and indexing is not supported for DB2.

- By default, DB2 databases use a 4 KB page size. Some related products (including Collaboration Manager and Content Tracker) require a 32 KB page size. If you intend to install any of these products on the content server, you should increase the page size for DB2 to 32 KB *before* installing the Content Server software. Otherwise, you need to drop and re-create the content server tables using a 32 KB page size before installing Collaboration Manager or Content Tracker on the content server. Please note that this will wipe out any data already in the database tables, so make sure that you properly back up the data before dropping the database tables. You can then restore the data after re-creating the tables.

- DB2 does not support dropping of database fields. If a field is deleted from a table, the entire content of the database table needs to be dumped into a temporary table. The table then needs to be re-created and the data dumped back into the new database table. The table indexes cannot be re-created. This means that if you add a custom metadata field to a Content Server database table using Configuration Manager and then delete that field at some point, any indexes to custom fields in the database table are removed from the database, even if those custom fields are unrelated to the field that was deleted.

3.6 Search Solutions

Please note the following considerations for the search solutions supported by Content Server 10*g*R3:

- For more information about the search solutions that can be used with Content Server 10*g*R3, refer to "Search Solutions" on page 2-9.

- For a number of considerations related to database search and indexing, refer to "All Databases" on page 3-6.

- For more information about setting up the database for full-text searching and indexing, refer to Appendix D, "Setting Up Database Search and Indexing."

- If you are upgrading to Content Server 10*g*R3 from an earlier Content Server release with Verity, then the Verity search engine will continue to work after the upgrade to release 10*g*R3. See "Migrating From Verity to Database Searching/Indexing" on page 6-7 if you want to switch to database searching and indexing after updating your Content Server instance.

3.7 JDBC Drivers and Settings

A JDBC driver is required for Content Server to connect and interact with the database. A default JDBC driver is provided for some databases, but you can also

choose a custom JDBC driver. For some databases, you are required to provide your own JDBC driver. The JDBC requirements and defaults depend on the database that is used with the content server:

- Oracle

- Sybase

- SQL Server

- DB2

3.7.1 Oracle

The following default JDBC driver settings are used for Oracle:

- **JDBC driver classname:** oracle.jdbc.driver.OracleDriver

- **JDBC driver is installed from:** \packages\allplatform\oracle_jdbc\10.2.0.4.0\ojdbc14.jar

- **JDBC driver is installed to:** *[CS-Install]*\shared\classes\ojdbc14.jar

You are given the option during the Content Server software installation to use a custom JDBC driver.

3.7.2 Sybase

The following default JDBC driver settings are used for Sybase:

- **JDBC driver classname:** com.sybase.jdbc3.jdbc.SybDriver

- **JDBC driver is installed from:** \packages\allplatform\sybase_jdbc\jconn_6.0.5\jconn3.jar

- **JDBC driver is installed to:** *[CS-Install]*\shared\classes\ojdbc14.jar

You are given the option during the Content Server software installation to use a custom JDBC driver.

3.7.3 SQL Server

No JDBC driver for SQL Server is provided with the Content Server software. You need to obtain a JDBC driver yourself and have its files available during the software installation. You can use any JDBC 3.0 compliant driver for SQL Server that runs on the Java Runtime Environment (JRE) 1.4 and later versions. The following driver has been tested and found to work reliably with Content Server:

- **jTDS driver**: This is an open-source JDBC driver for Microsoft SQL Server (both 2000 and 2005) which provides a complete implementation of the JDBC specification. You can download the jTDS driver from http://jtds.sourceforge.net.

    Specify the following information when prompted during the Content Server installation:

    - **JDBC driver classname:** net.sourceforge.jtds.jdbc.Driver

    - **JDBC connection string:** jdbc:jtds:sqlserver://*[DB-Host]*:*[Port]*/*[DB-Name]*

3.7.4 DB2

There are no redistributable JDBC drivers for DB2, and that is why you must always specify one manually for this database. You will typically use the following two Universal JDBC driver files for DB2:

- *[DB2-Dir]*/sqllib/java/db2jcc.jar

- *[DB2-Dir]*/sqllib/java/db2jcc_license_XX.jar

[where 'XX' is a two-letter code for the platform (typically 'CU' for Windows)]

Copy the jar files to a directory on the machine on which the content server is being installed. This is the path you will specify for the JDBC drivers during the Content Server software installation.

3.8 Accessibility of the Content Server Interface

Pursuant to Oracle's commitment to accessibility in all of its applications, accessibility issues are addressed for this version of Content Server, including the following:

- the top menu and tray menu interfaces are now fully accessible via keyboard and can be seen by screen readers as well. To implement this change, make sure to install the CoreUI and YahooUserInterfaceLibrary components and set `EnableAccessibilityMode=1` in the config.cfg file.

- color-dependent indications of required fields are now supplemented with an asterisk (*) to indicate the field is required

- summaries are available for all tables

- pages are now set to a primary language

- labels have been added to form fields

- multi-select options are now accessible via the keyboard

- a 'skip to content' navigation link is provided

- alternate tags are now available for all images

Note: Note that all of these changes are currently in the core Content Server only. Components may not yet be compliant.

4

Installing a New Content Server

The installation procedure for a new Content Server instance depends on the preferred installation method:

- Command-Line Installation: With this installation method, the Content Server software is installed using a text-based, command-line interface.

- Unattended Installation: With this installation method, the Content Server software is installed using script files, which are executed by the installer without any intervention by the user.

> **Important:** Prior to installing on Windows Server 2008 R2 (64-bit), you must download and install a 64-bit Java virtual machine. After installing a 64-bit JVM, you must then prepare the Content Server installation files for use on a 64-bit system by running the PreInstaller.bat file located in the GenericPreinstaller directory of the distribution media. Running the PreInstaller.bat prepares the installation files and then begins the installation process.

4.1 PreInstallation for 64-bit System

To install Content Server on a 64-bit system using either the command-line or unattended installation options, you must first:

1. obtain and install a 64-bit Java virtual machine

2. initiate the installation using the PreInstaller.bat file instead of the standard install.exe file

The Sun JDK version 1.6.0_25 (64-bit) was used when testing a Content Server installation on a Windows Server 2008 R2 (64-bit) system. Note that you must manually enter a path to the custom JVM when prompted during installation. For example, `c:/jdk1.6.0_25/bin/java.exe`

The PreInstaller.bat file is located in the GenericPreinstaller directory of the distribution media. It prepares the installation files for a 64-bit system and initiates the installation process.

4.2 Command-Line Installation

With this installation method, the new content server is installed using a text-based, command-line interface.

Important Considerations

Please note the following:

- The installation procedure contained in this document assumes that you install Content Server on the same system as the web server. See Appendix F, "Disassociated Installations" for more information about installing the content server on a different computer than the web server.

- Throughout the installation procedure described below, you may press [Enter] to accept the default, which is indicated either by square brackets ([ ]) or an asterisk (*).

- Whenever you need to specify a path, make sure that you use forward slashes (/), for example *c:/company/idcm1*.

- You can abort the installation procedure at any point by pressing Ctrl+C.

Installation Procedure

To install a new content server using the command-line interface, complete the following steps:

1. Obtain the Content Server software distribution package for Microsoft Windows.

2. If you obtained the software distribution package as a zip file, unzip the file to a temporary installation location.

   > **Important:** Make sure that you do not unzip or copy the installation files to a directory that contains any spaces (for example, *C:\CS Install*) and start the installation from there. If you do, the installation process may not complete successfully and may hang under certain circumstances.

   If you downloaded an ISO image, either burn a CD or mount the ISO image to access the installation files.

   If you have a software distribution CD, insert it in the CD or DVD drive.

3. Open a command prompt window and navigate to the *\UCM\ContentServer\win32* directory of the installation location.

4. Enter `Installer` and press [Enter].

   > **Note:** You can specify some command-line parameters for the installer to override a number of default installation settings. For example, you may turn off the initial system checking that takes place by default. For further details refer to "Overriding Script File Entries" on page E-11.

   > **Note:** Throughout the installation, when entering a text value, you can press Enter to accept the default that appears between square brackets ([ ]). When selecting from a list, you can select the choice preceded by an asterisk (the default) by pressing Enter.

5. You are prompted to choose the **language** of the installation procedure. Select a language from the list, and press [Enter].

6. You can now select from a menu of **installation options**. Press '1' and [Enter] to install a new content server.

7. You are prompted to enter the full path to the target **installation directory** for the new content server. Specify a valid installation directory path or accept the default, and press [Enter] when you are done. If you specify a directory that does not yet exist, you are asked whether this directory should be created. Press '1' (or [Enter]) to confirm.

> **Note:** If you are planning to install multiple Content Server instances on the same computer, you must use separate directories for each instance.

> **Important:** The directory path should not contain any spaces.

8. You are prompted to specify what **Java Virtual Machine (JVM)** will be used with the new content server. If you press '1' or [Enter], the Sun JVM version 1.5.0_11 is installed. If you press '2', you can specify a custom JVM 1.5 by typing the full path name to the JVM executable and pressing [Enter].

> **Important:** If installalling on a Windows Server 2008 R2 (64-bit) system, you must download, install, and specify a 64-bit custom JVM, such as the Sun JDK version 1.6.0_25 (64-bit).

9. You are prompted to specify the location of the **native file repository** (the Vault) for the new content server. This is where Content Server stores the native files checked in by contributors. Specify a valid directory path or accept the default, and press [Enter] when you are done. If you specify a directory that does not yet exist, you are asked whether this directory should be created. Press '1' (or [Enter]) to confirm.

> **Important:** The directory path should not contain any spaces.

10. You are prompted to specify the location of the **web-viewable file repository** (the Web Layout) for the new content server. This is where Content Server stores the web-viewable versions of the files checked in by contributors. Specify a valid directory path or accept the default, and press [Enter] when you are done. If you specify a directory that does not yet exist, you are asked whether this directory should be created. Press '1' (or [Enter]) to confirm.

> **Important:** The directory path should not contain any spaces.

11. You are prompted to specify the **authentication setup** of the new content server. A server can be configured to manage its own authentication (as a master server) or to allow another master to act as an authentication proxy. Select an option and press [Enter] to continue.

> **Note:** If you choose to let another server instance manage the authentication, the new content server is effectively a proxied server instance.

> **Tip:** Proxied servers for Content Server 10*g*R3 differ from proxied servers for earlier releases in that they do not share the shared directory with their associated master. This means that 10*g*R3-style proxied servers take up much more disk space than pre-10*g*R3 proxied servers and take longer to install.

12. If you chose to have another master to act as an authentication proxy for the new content server, complete this step. Otherwise, skip this step and continue with step 13.

You are prompted to specify the path to the master server that should handle the **authentication for the new content server**. Enter the server's full directory path, and press [Enter] to continue. If you specify an invalid path, you are prompted to enter the path again.

13. You are prompted to specify whether an **administration server** should be installed and configured to manage the new content server. You can set up a new admin server for the new content server. If there is already an admin server on the system, you may choose to configure that admin server to administer the new content server. You may also choose not to configure an admin server at all. Select an option and press [Enter] to continue.

> **Note:** If you choose not to install an admin server, you will not be able to perform administrative tasks remotely using a web browser interface. Any system administration work then needs to be done on the computer running the content server itself.

14. If you choose to use an existing admin server for the new content server, complete this step. Otherwise, skip this step and continue with step 15.

You are prompted to specify the path to the **admin server that should manage the new content server**. Enter the server's full directory path, and press [Enter] to continue. If an existing master server is detected, the path defaults to that server's admin server. If you specify an invalid path, you are prompted to enter the path again.

15. You are prompted to specify the location of your **web browser executable**. This browser will be used to display the online help (if called on the same computer as the content server). Specify the location path of your browser of choice or accept the default, and press [Enter].

16. You are prompted to specify the **system locale** for the new content server. The system locale defines how the content server handles a number of language-specific issues such as date/time format, default time zone, and default interface language (if a localized user interface is available). For further details on the system locale refer to the *Using Content Server in International Environments* guide. Select the system locale from the list, and press [Enter].

> **Note:** The system locale of a content server instance can be changed at any time using the System Properties utility.

17. You are prompted to specify the **time zone** in which the new content server will operate. Accept the default (Use the time zone setting for your operating system) or select a world region, and press [Enter].

18. If you chose not to use the time zone setting of the operating system, complete this step. Otherwise, skip this step and continue with step 22.

You are prompted to specify in which time zone the content server will operate. Choose the time zone from the list, and press [Enter]. If the displayed list does not include your time zone, you can press 'm' for more choices.

19. You are prompted to enter the **content server port number** of the new content server. This port must be otherwise unused, and must be unique for each content server instance on the same computer (master or proxied). Specify the port number, or press [Enter] to accept the default. If you specify a port number that is already in use by another content server instance, you are prompted to enter the port number again.

20. If you chose to use a separate admin server for the new content server in step 13, complete this step. Otherwise, skip this step and continue with step 21.

You are prompted to enter the **administration server port number** of the new content server. The Admin server enables administrators to perform a number of system administration tasks for the content server from a remote location using a web browser interface. The specified port must be otherwise unused, and must be unique for each instance on the same computer. Specify the port number, or press [Enter] to accept the default. If you specify a port number that is already in use by another content server instance, you are prompted to enter the port number again.

21. You are prompted to specify the **security filter** of the new content server. This filter is used to restrict access to the content server. Only hosts with IP addresses matching the specified criteria are granted access to the content server. The default is 127.0.0.1 (localhost), but you can add any number of valid IP addresses. You can specify multiple IP addresses separated by the pipe symbol (|), and you can use wildcards (* for zero or many characters, and ? for single characters).

Example: 127.0.0.1|10.10.1.10|62.43.163.*|62.43.161.12?

If you use any of the products below, you need to make sure the incoming connection address filter includes the network IP address of the computer that these products are running on, even if this is the same physical computer that is also hosting Content Server:

- Report Parser
- Content Integration Suite (CIS)
- Content Categorizer
- Inbound Refinery (IBR)
- Content Server JavaBeans (IdcServerBean, ContentServerBean, ServerBean)
- Customizations that communicate with Content Server via IdcCommand or IdcCommandUX
- Other Content Server instances that wish to communicate via sockets

In the situations below, the security filter needs to include the IP address of the remote computer:

- The web server and the content server are on different systems (see Appendix F, "Disassociated Installations"). (You then need to add the IP address of the web server.)

- There are EJB-enhanced operations. (You then need to add the IP address of the remote server.)

- The IdcCommand or IdcCommandUX utility is used on a system separate from the content server. (You then need to add the IP address of the web server.)

Make sure that the security filter always includes the localhost IP address (127.0.0.1), in addition to any other IP addresses.

If you do not specify the security filter correctly, this may result in significant errors for routine functions.

The security filter does not restrict browser access to the content server; it only limits access when using the technologies mentioned above.

After installing the Content Server software, you can always modify the security filter on the Server tab of System Properties.

> **Important:** Make sure that you specify the computer's real network IP address for the above products. If the product is running on the same computer as Content Server, the localhost IP address (127.0.0.1) is not sufficient.

When you are done, press [Enter].

22. You are prompted to specify the **URL prefix (web server relative root)** of the new content server. Specify the web server relative root or accept the default, and press [Enter] when you are done. If you specify a URL prefix that is already in use by another content server instance, you are prompted to enter the URL prefix again.

This URL prefix is used when generating HTML pages that refer to the contents of the *weblayout* directory within the installation. This prefix must be mapped in the web server to the physical location of the *weblayout* directory.

For an installation with multiple content server instances, make sure that the URL prefix (web server relative root) is different for each server instance.

> **Important:** If you plan to use Enterprise Search, make sure that you use different web roots for each content server instance (for example, Server1, Server2, etc.). Otherwise you must make modifications to the configuration of each content server instance to provide them with a unique relative web root (HttpRelativeWebRoot value). Enterprise Search will not work if all content server instances have identical web root directory names. It is recommended that you contact support if you have already installed a content server instance and need to change its web root.

23. You are prompted to specify the name of the **local mail server** for the new content server. Specify the name using the following format: *mail.companyname.com*. The

content server will contact this system to deliver e-mail. Press [Enter] when you are done.

24. You are prompted to specify the **e-mail address of the Content Server system administrator**. Specify the e-mail address, and press [Enter] when you are done.

25. You are prompted to specify the **web server HTTP address** for the new content server. Specify the HTTP address of your web server (for example *web.company.com*) or accept the default (which is the detected computer name), and press [Enter] when you are done.

The address specified here will be used when generating HTML pages. For example, *web.company.com* could be used in your installation to refer to the URL *http://web.company.com/root* (where 'root' would be the web server relative root; see step 22).

> **Important:** If your web server is running on a port other than 80, you need to append a colon and the port number to the HTTP address (for example, *web.company.com:81*).

26. You are prompted to specify a **name** for the new content server instance you are installing. This name should be unique across the entire enterprise; the name may not contain characters other than letters, numbers, and underscores. Specify the name or accept the default, and press [Enter] when you are done.

27. You are prompted to specify a **short label** for the new content server instance (for example, *server_2*). This label is used on web pages to identify this instance. The maximum number of characters for the label is 12. Specify the label, and press [Enter] when you are done.

28. You are prompted to specify a **long description** for the new content server instance. Specify the description (for example, *Content Server server_2*), and press [Enter] when you are done.

29. You are prompted to specify the **web server** that will be used with the new content server. A list of supported web servers is provided. You may also choose to configure the web server manually. Select an option from the list and press [Enter] to continue.

> **Note:** For Sun ONE, do not forget to carry out the post-installation tasks (see Chapter 5, "Post-Installation Tasks and Considerations").

If you choose to configure the web server manually, refer to Appendix A, "Setting Up Your Web Server" for more information on the manual configuration process.

30. If you selected Microsoft IIS 5.0/6.0 as the web server in step 29, complete this step. Otherwise, skip this step and continue with step 32.

If **file handling caching** is enabled, you are prompted to specify whether it should be disabled. This is recommended so that locked files on your Web site can be updated dynamically without conflict from the web server. Press '1' (yes) or '2' (no), and press [Enter] to continue.

31. If you selected Microsoft IIS 5.0/6.0 as the web server in step 29, complete this step. Otherwise, skip this step and continue with step 32.

You are prompted to specify what **security integration** should be used for IIS:

- **Standard security**: Set up standard security manually. User, role, and account information must be set up separately from Windows NT security.

- **NTLM security**: Choose this option only if Microsoft Internet Explorer is used in conjunction with IIS. User, role, and account information are mapped from Microsoft network security. This is beneficial for sites desiring a single source of user administration and for complex security models. For this option, the server on which you install the core components must be participating in a Microsoft network security domain. It cannot be a stand-alone server or just a server participating in a workgroup. This means that if there are no other Microsoft network servers, your server must be a primary domain controller.

- **ADSI security**: Active Directory Services Interface (ADSI) is used to provide security.

Press '1' (standard), '2' (NTLM), or '3' (ADSI), and press [Enter] to continue.

32. If you selected Sun ONE as the web server in step 29, complete this step. Otherwise, skip this step and continue with step 33.

    You are prompted to specify the **full directory path** for the Sun web server to use with the new content server. Enter the web server's full directory path, and press [Enter] to continue.

    > **Note:** The directory you specify must contain a subdirectory called 'config' with the files *obj.conf* and *magnus.conf*. The installer will create new *obj.conf* and *magnus.conf* files in the *install* subdirectory of the installation directory. If possible, these files will be installed automatically. The original *obj.conf* and *magnus.conf* files will be renamed *install/obj.conf.orig* and *install/magnus.conf.orig*, respectively.

33. You are prompted to specify the **database** that will be used with the new content server. A list of supported databases is provided. You can choose between Oracle, SQL Server (2000 or 2005), Sybase, or DB2. You may also choose to provide custom JDBC settings or skip the database configuration completely and set it up manually (see Appendix B, "Setting Up Your Database").

    > **Important:** If you are using SQL Server 2008, you must opt to skip the database configuration at this time. Selecting any other option causes the installation to fail. After skipping database configuration and completing the installation, see Appendix B, "Setting Up Your Database" for steps to manually configure SQL 2008.

    Select an option from the list and press [Enter] to continue.

34. If you selected Oracle, Sybase, or DB2 in step 33, proceed with step 35.

    If you selected SQL Server (2000 or 2005) in step 33, proceed with step 36.

    If you chose to provide custom JDBC settings in step 33, proceed with step 36.

    If you chose to skip the database configuration in step 33, proceed with step 43.

35. You are prompted to specify whether you want to **manually configure JDBC settings** (i.e., the JDBC driver class name and JDBC connection string). Press '1' (yes) or '2' (no), and press [Enter] to continue.

You need to configure JDBC settings manually if you want to use a database JDBC driver other than the default ones provided with the software (see "JDBC Drivers and Settings" on page 3-13). If you are planning on using the default JDBC driver for a database, you will generally want to choose '2' (no).

If you selected 'yes', continue with step 36. If you selected 'no', continue with step 37.

36. You are prompted to specify the **JDBC driver class name**. Enter the driver class name and press [Enter], or press [Enter] to accept the default (if provided).

You are prompted to specify the **JDBC connection string**. Enter the connection string and press [Enter] when you are done.

> **Note:** See "JDBC Drivers and Settings" on page 3-13 for details on the default and supported JDBC drivers for the various databases.

37. You are prompted to specify some database settings. Some prompts may not be displayed depending on your choices in earlier database configuration steps. For example, if you specified a custom JDBC connection string, you may not be prompted for the database name, server name, and/or port number (since this information is included in the connection string).

- You are prompted to specify the **database server host name**. Enter the server name, or press [Enter] to accept the default, if provided.

- You are prompted to specify the **database port number**. Enter the port number, or press [Enter] to accept the default, if provided.

- You are prompted to specify the **database user name** that is used by the new content server to log into the database. Enter the database user name, or press [Enter] to accept the default, if provided.

- You are prompted to specify the **database user password** that is used by the new content server to log into the database. Enter the database password, and press [Enter] to continue. Please be aware that for security reasons, no characters are displayed on screen in the command window when entering the password.

- You are prompted to specify the **database or instance name**. Enter the database or instance name, or press [Enter] to accept the default, if provided.

38. If you selected Oracle or Sybase as the database in step 33 or chose to provide custom JDBC settings, complete this step. Otherwise, skip this step and continue with step 39.

You are prompted to specify whether the JVM should be configured to **find the JDBC driver in a specific jar file**. Press '1' (yes) or '2' (no), and press [Enter] to continue.

39. If you selected SQL Server or DB2 as the database in step 33 or chose to point to a specific JDBC driver jar file in step 38, complete this step. Otherwise, skip this step and continue with step 41.

You are prompted to specify the **JDBC driver jar file path**. Enter the full path(s), including the jar file name(s), and press [Enter] when you are done. For example:

```
C:/jtds/jtds.jar
```

> **Note:** Make sure that you use forward slashes (/) to separate directories in a path. Also, if you need to specify more than one file, you can separate them using semicolons: *[Path1]/[File1];[Path2]/[File2];* etc.

No default JDBC drivers for SQL Server and DB2 are provided with the Content Server software, and that is why you always need to specify one manually for these databases. See "JDBC Drivers and Settings" on page 3-13 for more information about supported JDBC drivers for SQL Server and DB2.

40. You are prompted to specify whether the **JDBC driver files should be copied**. Press '1' (yes) or '2' (no), and press [Enter] to continue.

If you choose 'yes', the JDBC driver files will be copied to *[CS-Install]\shared\classes*.

41. You are prompted to specify whether the installer should attempt to **create the database tables automatically**. Press '1' (yes) or '2' (no), and press [Enter] to continue.

42. You are prompted to specify whether **Unicode text fields** (UCS-2) should be used in the database. If you choose not to, the native database field encoding will be used. Press '1' (yes) or '2' (no), and press [Enter] to continue.

Unicode text fields in the database are generally recommended if the content server needs to handle content in Asian or bidirectional languages (for example, Japanese, Korean, Arabic, and Hebrew) or may do so in the future. Unicode text fields give you more flexibility as the database can handle virtually any language, but it does double the size of the database since every character is represented as two bytes rather than one.

If you choose native database encoding, the 'varchar' data type is used for the database columns created for the content server. If you choose Unicode encoding, the 'nvarchar' data type is used.

Choosing Unicode encoding does not affect the language encoding, or charset, of the database. It only affects the data types of the database columns created for the content server ('nvarchar' rather than 'varchar'). Also, the data encoding for the Content Server database does not apply to the entire enterprise database, but only to Content Server's reserved tablespace within that database.

43. You are prompted to specify what optional components should be enabled with the new content server. These components add functionality to the base content server. You can choose from the following components:

- AddCCToArchiveCheckin
- AddCCToNewCheckin
- ContentCategorizer
- ContentFolios
- ContentTracker
- ContentTrackerReports
- ExtendedUserAttributes
- Folders_g
- LinkManager8

- OracleTextSearch

- PDFWatermark

- ThreadedDiscussions

> **Note:** See Appendix C, "Content Server Components" for more information on each of these components.

In addition to these optional components, a number of other components are always installed with the Content Server software. See Appendix C, "Content Server Components" for further details.

You can toggle a component's installation status by typing its associated number. A currently unselected component is then marked for installation, and vice versa. You use commas to separate multiple components, for example: `1,3`. The installation selection of each of these components is then reversed. To unselect all components enter 0.

Type '`f`' (for Finish) when you are done, and press [Enter] to continue.

> **Note:** The component zip files are all located in the *packages\allplatform* directory of the software distribution package. If you choose not to install a particular component at this point, you can always install it later from this location using the normal methods. See the Content Server administration documentation for more information on installing and enabling components.

44. You are prompted to specify how the **Admin Server service** should be configured. You may choose to install the service and start it automatically, just install it (and start it manually), or not install it at all. Select an option and press [Enter] to continue.

> **Note:** If you choose not to install the service, you will not be able to perform administrative tasks remotely using a web browser interface until you start the admin server (if you chose to install it in step 13).
>
> If you choose not to install the service but decide to install it at a later time, open a command window, navigate to the *<InstallDir>*\bin directory, then run the following commands:
>
> ```
> IdcAdminNT -install
> IdcServerNT -install
> ```
>
> Similarly, if you install the service and need to uninstall it from the command line, open a command window, navigate to the *<InstallDir>*\bin directory, then run the following commands:
>
> ```
> IdcAdminNT -uninstall
> IdcServerNT -uninstall
> ```

45. If you chose to run the Admin Server service automatically, complete this step. Otherwise, skip this step and continue with step 47.

You are prompted to specify whether the service should **run as a specific user**. Press '1' (yes) or '2' (no), and press [Enter] to continue.

If you choose 'No', the Admin Server service will be set up to run as 'localhost'.

> **Note:** The correct syntax for defining a specific user takes the following form:
>
> - Local user syntax is: username=.\[username]
>
> - Domain user syntax is: username= [domain]\[username]

46. If you chose to run the Admin Server service as a specific user, complete this step. Otherwise, skip this step and continue with step 47.

You are prompted to specify the **name** of the user that the Admin Server service should run as. Enter the name, and press [Enter] when you are done.

You are prompted to specify the **password** of the user that the Admin Server service should run as. Enter the name, and press [Enter] when you are done.

47. You are prompted to specify whether the Admin Server service should be **dependent on another service**. This is useful in situations in which the service should not start until another service is running. Press '1' (yes) or '2' (no), and press [Enter] to continue.

> **Important:** SQL Server *must* start before Content Server. If you are using SQL Server, make sure that you press '1' (yes). You may also choose to set this up manually after the Content Server installation (see "Starting SQL Server Before Content Server" on page 5-7).

48. If you chose to make the Admin Server service dependent on another service, complete this step. Otherwise, skip this step and continue with step 49.

You are prompted to specify the **Admin Server service dependency** (i.e., the name of the service that needs to run before the Admin Server service will be started). Enter the service name, and press [Enter] when you are done.

> **Note:** For SQL Server, specify `MSSQLServer`.

49. You are prompted to specify how the **content server service** should be configured. You may choose to install the service and start it automatically, just install it (and start it manually), or not install it at all. Select an option and press [Enter] to continue.

> **Note:** If you choose not to install the service, you can only start the content server as an application (by selecting from the **Start** menu, **Programs**, then **Content Server-[Instance Name]**, and then **Content Server**).

50. If you chose to run the content server service automatically, complete this step. Otherwise, skip this step and continue with step 52.

You are prompted to specify whether the service should **run as a specific user**. Press '1' (yes) or '2' (no), and press [Enter] to continue.

> **Note:** If you choose 'No', the content server service will be set up to run as 'localhost'.

> **Note:** The correct syntax for defining a specific user takes the following form:
>
> - Local user syntax is: username=.\[username]
>
> - Domain user syntax is: username= [domain]\[username]

51. If you chose to run the content server service as a specific user, complete this step. Otherwise, skip this step and continue with step 52.

You are prompted to specify the **name** of the user that the content server service should run as. Enter the name, and press [Enter] when you are done.

You are prompted to specify the **password** of the user that the content server service should run as. Enter the name, and press [Enter] when you are done.

52. You are prompted to specify whether the content server service should be **dependent on another service**. This is useful in situations in which the content server service should not start until another service is running. Press '1' (yes) or '2' (no), and press [Enter] to continue.

> **Important:** SQL Server *must* start before Content Server. If you are using SQL Server, make sure that you press '1' (yes). You may also choose to set this up manually after the Content Server installation (see "Starting SQL Server Before Content Server" on page 5-7).

53. If you chose to make the content server service dependent on another service, complete this step. Otherwise, skip this step and continue with step 54.

You are prompted to specify the **content server service dependency** (i.e., the name of the service that needs to run before the content server service will be started). Enter the service name, and press [Enter] when you are done.

> **Note:** For SQL Server, specify `MSSQLServer`.

54. You are prompted to specify whether the **8.3 file name creation** should be disabled for the new master content server. Press '1' (yes) or '2' (no), and press [Enter] to continue.

> **Note:** This prompt is shown only if 8.3 file name creation is not already turned off on the content server computer.

For systems dedicated to running Content Server, disable the 8.3 naming convention. This ensures that long file names in the native file repository directory (vault) and web viewable file repository directory (weblayout) are not compressed using a tilde (~). All systems used for production purposes should be dedicated to running Content Server.

For systems not dedicated to running Content Server, do not disable the 8.3 naming convention option. This ensures that other products installed on this system which require the 8.3 naming convention function properly. Systems not dedicated to running Content Server could be demonstration or development systems.

If you choose not to disable the 8.3 naming convention, avoid any document names (dDocName) that are exactly six characters in length. Otherwise there could be file names such as *xxxxxx~1.pdf*, which can be equivalent to the 8.3 file name generated for a web-viewable rendition of *xxxxxxyyy.pdf*. This can happen with renditions that have the same extension as the web-viewable file (for example, thumbnails of jpeg files) or when a document with six characters is a prefix for a document name that is longer. If you make sure that your autonumbering has a non-empty prefix, then it is highly unlikely that 8.3 file naming will cause any issues.

55. The installer now performs a number of pre-installation checks. If there are any errors or warnings, they are reported. Review the installation settings, and then indicate whether the installation should proceed or abort, or whether you want to make changes to the configuration. You can also recheck the configuration. This enables you to correct any reported errors before proceeding. When you are ready, choose a menu option and press [Enter] to continue.

If you chose to proceed with the installation, all files are copied and the configuration settings made. During that process, a message line shows the percentage of what has been completed, as well as a brief description of the task currently being performed.

4.3 Unattended Installation

Content Server supports unattended installations. They are basically command-line installations with a specific script file as the parameter. This enables administrators to install and set up the Content Server software on multiple computers using the exact same installation settings, without any human intervention (other than starting the installation process).

The following topics are important with regard to unattended installations:

■   "Creating a Script File" on page 4-14

■   "Running an Unattended Installation" on page 4-15

4.3.1 Creating a Script File

Before you can perform an unattended installation, you need a script file that contains all the required installation parameters. The easiest way to create this file is to go through a new installation of a content server all the way to the final review step. Do not proceed at this point! Rather, abort the installation and go to the *[CS-Install]\install* directory. The installer generated a script file that was going to be used to install the Content Server software. The generated script file is named *[date]-[type].txt*, where [date] is the current date and [type] the type of installation ('new', 'update', 'proxy'), for example *2008-04-21-new.txt*. Please note that the date is always formatted as YYYY-MM-DD.

Once a script file has been created, it can easily be modified and reused.

> **Note:** Refer to Appendix E, "Installation Script Files" for further details on creating and modifying script files.

4.3.2 Running an Unattended Installation

To install a new content server using an unattended installation, complete the following steps:

1. Obtain the Content Server software distribution package for Microsoft Windows.

2. If you obtained the software distribution package as a zip file, unzip the file to a temporary installation location.

   > **Important:** Make sure that you do not unzip or copy the installation files to a directory that contains any spaces (for example, *C:\CS Install*) and start the installation from there. If you do, the installation process may not complete successfully and may hang under certain circumstances.

   If you downloaded an ISO image, either burn a CD or mount the ISO image to access the installation files.

   If you have a software distribution CD, insert it in the CD or DVD drive.

3. Open a command prompt window and navigate to the *\UCM\ContentServer\win32* directory of the installation location.

4. Enter `Installer` followed by the name of the script file to be used (including the full path, if required), for example:

   ```
   Installer  c:\scripts\install.txt
   ```

   > **Note:** You can also specify some command-line parameters for the installer to override a number of default installation settings. For example, you may turn off the initial system checking that takes place by default. For further details on the available command-line parameters refer to Appendix E, "Installation Script Files."

5. Press [Enter] to start the unattended installation.

6. The installer now analyzes the script file. If it finds no fatal errors, it starts installing the software based on the parameters contained in the installation script file. During that process, a message line shows the percentage of what has been completed, as well as a brief description of the task currently being performed.

   Any errors that occur after the initial pre-installation check are recorded in a log file called *log.txt*, which is located in the *[Master_Dir]\/install* directory. The file is a plain-text file that can be opened and edited using any text editor such as Notepad or WordPad.

   > **Note:** For further details on installation script files, including the available script file entries, refer to Appendix E, "Installation Script Files."

5

Post-Installation Tasks and Considerations

Depending on the selected installation options, there may be some tasks that need to be performed *after* installing the Content Server software. They are related to the following:

5.1 Installation Log File

After performing a command-line installation, it is recommended that you check the installation log file (*log.txt*), which is located in the directory *[CS-Install]\install* (where *[CS-Install]* is the installation directory of the content server instance). If any errors or warnings occurred during the installation, they will be logged in this file.

5.2 Windows Server 2008 R2 (64-bit) Installation Clean-Up

Once installation is completed successfully, you must point Content Server to the 64-bit JVM:

1. Open the intradoc.cfg file located in the [*CS-Install*]/bin/ directory in a standard text editor and set the JDK_custom configuration equal to the location of the bin directory that contains the Java executable installed with the JDK. For example, if the java.exe file installed with the 64-bit JVM is located at `C:\jdk_1.6.0_25\bin\java.exe`, then set the JDK_custom configuration as follows:

   ```
   JDK_custom=C:\jdk_1.6.0_25\
   ```

2. Save changes and close the intradoc.cfg file.

3. Restart the Content Server.

5.3 Date Format

The default English-US locale uses two digits to represent the year ('yy'), where the year is interpreted to be between 1969 and 2068. In other words, 65 is considered to be 2065, not 1965. If you want years prior to 1969 to be interpreted correctly in the English-US locale, you need to change the default date format for that locale to use four digits to represent years ('yyyy').

> **Note:** This issue does not apply to the English-UK locale, which already uses four digits for the year.

To modify the default English-US date format, proceed as follows:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Localization tab.

3. Select the English-US entry in the list of locales, and click **Edit**.

   The Configure Locale dialog is displayed.

4. Modify the date format to use four digits for the year ('yyyy') rather than two ('yy').

5. After you are done editing, click **OK** to close the Configure Locale dialog.

6. Click **OK** to apply the change and exit System Properties.

7. Stop and restart the Content Server (otherwise the change will not take effect).

5.4 Time Zone

During the installation of the Content Server software, you may have indicated that you wanted to use the default time zone for the selected system locale. If that is the case, the installer attempted to automatically detect the time zone of the operating system and set the Content Server time zone accordingly. In certain scenarios, the time zone of the operating system may not be recognized. The time zone will then be set to the UTC time zone (Universal Time Coordinated), which is the same as Greenwich Mean Time (GMT).

You then need to set the time zone manually. To do this, proceed as follows:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Server tab.

3. From the System Timezone drop-down list, choose the time zone you want to use for the current content server instance.

4. Click **OK** to apply the change and exit System Properties.

5. Stop and restart the Content Server (otherwise the change will not take effect).

5.5 International Environments

Content Server fully supports multilingual, international environments:

- It can be installed on non-English (including Asian) operating systems.

- It can handle and store content in a large number of languages.

- It can create a full-text index of content in a large number of languages.

- It can be set up to offer localized end-user environments.

Depending on the content server setup and multilingual requirements, some of the settings of the default installation may need to be modified, including:

- The **system locale** of the content server, which defines how that content server handles a number of language-specific issues such as the date/time format, default time zone, sort order, and default interface language.

- the **Verity locale** of the content server (if applicable), which is used to make sure language-specific characters in text are indexed correctly.

UTF8 File Encoding

Non-7-bit ASCII characters are allowed in filenames but are not supported in user names. The Content Server installation process now automatically sets File Encoding to UTF8. If non-7-bit ASCII characters are needed in user names, the ExtranetLook component must be used to facilitate cookie logins.

Setting FileEncoding to a value other than UTF8 is not a supported configuration. Therefore, the suggested process for enabling non-7-bit ASCII characters in user names is to use the ExtranetLook component and cookie login.

For full details on deploying an content management system in international, multilingual environments, refer to the document *Using Content Server in International Environments*. This document is part of the Content Server product documentation, which can be accessed through the online Help. It is also available as a PDF file in the Content Server documentation distribution package (*integrator\internat_ environments_10en.pdf*).

> **Important:** Is it strongly recommended that you make any configuration changes to the content server before any content is checked in. If you make changes with content already checked in, the search index needs to be rebuilt, which can be quite a lengthy process (depending on the number of checked-in content items).

5.6 Localized User Interfaces

Content Server 10*g*R3 supports the following end-user interface languages:

- English

- German (Deutsch)

- French (Français)

- Dutch (Nederlands)

- Spanish (Español)

- Italian (Italiano)

- Japanese

- Korean

- Chinese (both traditional and simplified)

- Thai

- Arabic

> **Note:** The administration sections of the Content Server environment may not be localized into all of these languages.

The user interface language is automatically set to match the locale of the operating system, although end-users can choose their preferred user interface language from their user profile page. Please note that the software help is in English, regardless of the Content Server user interface language.

All files required to provide localized user interfaces for Content Server 10*g*R3 are installed along with the Content Server software. System administrators need to explicitly make a language available to end-users before they can select it in their user profile. To enable user interface languages, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Localization tab.

3. In the list of locales, select the user interface language(s) you want to make available to end-users, and click **Enable**. You can select multiple locales by holding the Shift key (consecutive selection) or Ctrl key (non-consecutive selection) while clicking on the locale entries.

4. When you are done, click **OK** to apply the setting and exit the System Properties utility.

5. Restart each instance of the content server.

   End-users can now select their preferred user interface language on their user profile page.

> **Note:** In some situations, enabling locales on a Content Server installed on a native Japanese operating system can cause the interface to display in English. To correct this, open the config.cfg file in a standard text editor and add the variable `SystemLocale=Japanese`. The config.cfg file is located in the `<install_dir>/<instance_dir/config` directory.

5.7 Setting Up Your Search Solution

By default, Content Server 10*g*R3 is set up to use the database to provide searching and indexing capabilities. The out-of-the-box database configuration provides metadata-only searching and indexing. However, you can modify the default configuration of SQL Server and Oracle to enable full-text searching and indexing (Appendix D, "Setting Up Database Search and Indexing"). Sybase and DB2 only support metadata searching and indexing.

Add-ons are available which allow different search solutions to be integrated with Content Server (for example, Verity or FAST). Separate integration documentation is available for each supported search solution.

5.8 Active Virus Scanning and Content Server

To ensure smooth content server operation, it is recommended that you exclude the following Content Server directories from active virus scanning:

- [CS-Install]\weblayout\

- [CS-Install]\shared\

- [CS-Install]\data\

- [CS-Install]\search\

> **Important:** The *[CS-Install]\vault\~temp* directory should not be excluded, as it is the most important directory to scan.

If you feel that any of these directories need to be scanned, it is recommended that you run physical disk scanning on the Content Server computer during off-peak hours rather than actively scanning these directories. Also, for best results a local anti-virus program should be used to scan local drives.

5.9 Configuring Your Web Server

Depending on the web server and installation choices selected during the Content Server software installation, you may need to perform a number of tasks to set up and configure the web server for use with Content Server:

- Manual Configuration of the Web Server

- Sun Web Server Configuration Files

- Registering MIME Types for IIS 6.0

5.9.1 Manual Configuration of the Web Server

If, during the installation of the Content Server software, you chose to configure the web server manually, you need to perform a number of tasks to set up and configure the web server for use with Content Server. For further details refer to Appendix A, "Setting Up Your Web Server."

5.9.2 Sun Web Server Configuration Files

If, during the installation of the Content Server software, you chose to configure the Sun web server automatically, its configuration files were modified. You must apply these changes before they take effect.

To apply the changes to the Sun web server, complete the following steps:

1. Launch the Administer Web Server utility.

2. Enter the user name and password.

3. Select your server, and then click **Manage**.

4. A message is displayed indicating that changes were made to your configuration files. Click **OK**.

5. Click **Apply**, which is located in the top-right corner of the screen.

6. The Apply Changes page is displayed. Click **Load Configuration Files**.

7. A message is displayed confirming that your recent changes have been loaded.

8. Click **OK**.

9. Close the browser.

5.9.3 Registering MIME Types for IIS 6.0

For security reasons, IIS 6.0 will not serve a file if its file extension is not registered as a MIME type for the Web site. MIME (Multipurpose Internet Mail Extensions) is a standard used to communicate the type of data being delivered. When a file extension is not registered, IIS 6.0 returns a 404 (File not found) status code to the client browser. When this happens, it is recorded in the IIS logs with sc-status 404 and the scsubstatus 3. End-users experience any of the following:

- They cannot access a content item, even though it is there and they have access privileges to it.

- They cannot download content items of certain types (for example, AutoCAD files with file extension 'dwg' or log files with extension 'log').

- They cannot download content items with no file extension.

In order to prevent this from happening, you need to register the MIME types with IIS, so it will serve the associated files to the end-users. To do this, complete the following steps:

1. Start the Internet Information Services (IIS) Manager from Administrative Tools.

2. Bring up the Properties dialog for the server level object. The location and text for this object may be different depending on how the tool was started. In any view, it is the level above the Web Sites folder.

3. At the bottom of this dialog box, click the **MIME types…** button to bring up the MIME types dialog box. Here you can view, add, edit, remove file extension registrations for the entire server.

   Which MIME type to specify depends on the application. Typical settings for some common missing registrations are as follows:

File extension	MIME type
. (i.e., no file extension)	application/octet-stream
.log	text/plain
.dwg (i.e., AutoCAD drawings)	drawing/x-dwg

> **Note:** Note that the ability to add the file extension of just '.' to serve files without an extension was added in an update of Windows Server 2003. Using the no-extension registration is preferred over the wildcard extension (*). The wildcard extension would serve all unknown extensions and thus remove the security benefits of this IIS 6.0 feature.

4. Restart IIS.

5. Test the configuration. When the MIME type has been configured, you will be able to view or download the file.

> **Note:** If you prefer to change the configuration for a specific Web site, use the MIME types dialog on the HTTP Headers tab of the properties dialog for that site. At site level, the server-wide registrations do not display, making this harder to use.

5.10 Configuring Your Database

Depending on the database and installation choices selected during the Content Server software installation, you may need to perform a number of tasks to set up and configure the database for use with Content Server:

- Manual Configuration of the Database
- Starting SQL Server Before Content Server
- Preparing Sybase for Metadata Searching/Indexing
- Setting Up the Database for Full-Text Searching/Indexing

5.10.1 Manual Configuration of the Database

If, during the installation of the Content Server software, you chose to configure the database manually, you need to perform a number of tasks to set up and configure the database for use with Content Server. For further details refer to Appendix B, "Setting Up Your Database."

5.10.2 Starting SQL Server Before Content Server

It is necessary for SQL Server to start before Content Server starts. If you did not specify a service dependency during the Content Server installation, make sure that you run the file [*CS-Install*]\bin\IdcServerNT.exe (where [*CS-Install*] is the installation directory of the content server instance). This adds services required to start the servers in the correct order.

The syntax is as follows:

```
IdcServerNT -dependent [Name_of_Dependent_NT_Service]
```

If Content Server and SQL Server are installed on the same system, perform the following tasks:

1. Start a console window and navigate to the directory [*CS-Install*]\bin (where [*CS-Install*] is the installation directory of the content server instance).

2. Execute the following command:

```
IdcServerNT -dependent MSSQLServer
```

This command enables Content Server to start during the boot-up process, by enabling automatic as the startup type for the service.

> **Note:** The `-dependent` option cannot be used in combination with the `-install` option. Using the `-dependent` option without specifying a service name clears the current dependencies list.

5.10.3 Preparing Sybase for Metadata Searching/Indexing

If you chose Sybase as the database during the Content Server installation, it was configured to provide metadata searching and indexing. Sybase does not provide full-text indexing. After installing the Content Server software, make sure that you run the *rowlocking.sql* script (using *isql.exe*), if you did not already do so. This converts the Sybase database from table locking to row locking to reduce potential deadlock issues. This script is located in *[CS-Install]*\database\sybase\admin (where *[CS-Install]* is the installation directory of the content server instance).

5.10.4 Setting Up the Database for Full-Text Searching/Indexing

By default, Content Server 10*g*R3 is set up to use the database to provide searching and indexing capabilities. The out-of-the-box database configuration provides metadata-only searching and indexing. However, you can modify the default configuration of SQL Server and Oracle to enable full-text searching and indexing. This requires a number of manual configuration steps. For further details, refer to Appendix D, "Setting Up Database Search and Indexing."

> **Note:** Sybase and DB2 support metadata searching and indexing only.

5.11 Legacy Variable Definition when Upgrading from 7.x

When upgrading from a Content Server 7.x version, make sure that the CLASSPATH and JAVA_OPTIONS variables are commented out of the *[CS-Install]/bin/intradoc.cfg* file subsequent to upgrading. To comment out a variable, precede it with a # sign. For example:

6

Updating an Existing Installation

This section covers the following topics:

6.1 Supported Update Versions

The following Content Server versions can be upgraded directly to release:

- Content Server 7.*x* (both Verity and non-Verity editions)

- Content Server 10*g*R3

The above versions can *only* be upgraded to Content Server directly if they meet the hardware and software requirements in Chapter 2, "Installation Overview." If you need to upgrade your hardware and/or software (for example, the operating system), you will not be able to perform a direct update. Instead, you need to do a fresh installation (see Chapter 4, "Installing a New Content Server"). For example, if your current installation is running on Windows NT, you cannot upgrade to Content Server directly as this new release no longer supports this operating system. Similarly, a direct upgrade to Content Server is not supported if you are running MSDE or Informix as the database.

> **Note:** If you are updating a Content Server installation prior to release 10*g*R3 that includes proxied servers, these proxied servers will be updated as well and will continue to work as before.

6.2 Before You Begin

Carefully read Chapter 2, "Installation Overview" and Chapter 3, "Pre-Installation Tasks and Considerations" before beginning this section.

> **Note:** Either the 1.5 or 1.6 JVM is now required for update patches to 10.1.3.3.x releases.

Consider carefully the recommendations below, before updating an existing installation to Content Server 10*g*R3:

- The update procedure outlined in this section preserves all previous configuration settings for the master content server instance and all associated proxied instances.

- Make sure that your hardware and software meet all requirements laid down in Chapter 2, "Installation Overview." If they do not, upgrade them before updating the Content Server software. If you need to upgrade your hardware and/or operating system, you will not be able to perform a direct update to Content Server. Instead, you need to do a fresh installation (see Chapter 4, "Installing a New Content Server").

- It is strongly recommended that you create a fresh, full backup of your current instance (database and the entire installation directory structure) before performing the update procedure. Should anything go wrong during the update, you can then always revert back to the old configuration. For guidelines on backup strategies refer to the *Planning and Implementation Guide*.

  If the content server is running as an application, shut it down before updating the Content Server software. If the content server is running as a service, it does not need to be shut down. If the installer detects that the content server services are running during the update procedure, it will automatically shut them down and restart them after the update is complete.

- If you are running a content refinery module, check the Work in Progress page and wait until the refinery is not processing any content items. Once the refinery is done processing files, shut it down.

- Exit all applications (applets) before updating the Content Server software.

- Before running the installer for the Content Server update, make sure there are no browser connections to the content server.

- It is recommended that you disable all installed components before the upgrade and enable them one by one after the upgrade. This is a good strategy because it allows you to determine which components may have been broken by the upgrade. Please note that this is *not* necessary for the software upgrade as such to succeed; it is merely a useful customization upgrade strategy.

- There are dependencies between Content Server and installed components. If you update your Content Server instance, you should also update all installed components. Similarly, if you update any installed components, you should also update your Content Server instance with the latest patch sets. Prior to updating, make sure that your current components are compatible with the new Content Server release or that new, updated component versions are available.

  > **Important:** Not all pre-10*g*R3 components may be compatible with Content Server 10*g*R3.

- If any patches were applied to the content server (in the *[CS-Install]\classes* directory), these will be removed during the upgrade. Standard patches to the core content server are generally rolled into new releases of the Content Server software. Patches applied to custom components or older, still compatible extras or add-on products may need to be reapplied after a Content Server upgrade. Please contact Support if you have any questions about compatibility of patches not directly related to Content Server.

- Your content server will continue to run with the Java Virtual Machine (JVM) that it was using before the update.

- If you are upgrading to Content Server from an earlier release with Verity 4.5.1, then the Verity search engine will continue to work after the upgrade to release. If you want, you can switch to database searching and indexing (Chapter 6, "Updating an Existing Installation"). Please note that Content Server does not support Verity 2.7.

  When upgrading from a previous version of content server, and Verity is the search engine in use, set the following variable (as shown, in all caps) in the *[CS-Install]/config/config.cfg* file:

  ```
  SearchIndexerEngineName=VERITY.VDK.4
  ```

- Proxied server instances for Content Server 10*g*R3 take up much more disk space than proxied servers for earlier releases (Chapter 2, "Installation Overview"). This is because pre-10*g*R3 proxied servers share the *shared* directory with their master, whereas 10*g*R3-style proxied servers have their own *shared* directory. However, if you upgrade to Content Server from an earlier release, proxied servers will continue to share the *shared* directory with their master.

6.3 Updating a Content Server

To update an existing master content server to release 10*g*R3, complete the following steps:

1. Obtain the Content Server software distribution package for Microsoft Windows.

2. If you obtained the software distribution package as a zip file, unzip the file to a temporary installation location.

   > **Important:** Make sure that you do not unzip or copy the installation files to a directory that contains any spaces (for example, *C:\CS Install*) and start the installation from there. If you do, the installation process may not complete successfully and may hang under certain circumstances.

   If you downloaded an ISO image, either burn a CD or mount the ISO image to access the installation files.

   If you have a software distribution CD, insert it in the CD or DVD drive.

3. Open a command prompt window and navigate to the *\UCM\ContentServer\win32* directory of the installation location.

4. Enter `Installer` and press [Enter].

   > **Note:** You can specify some command-line parameters for the installer to override a number of default installation settings. For example, you may turn off the initial system checking that takes place by default. For further details refer to "Overriding Script File Entries" on page E-11.

> **Note:** Throughout the installation, when entering a text value, you can press Enter to accept the default that appears between square brackets ([ ]). When selecting from a list, you can select the choice preceded by an asterisk (the default) by pressing Enter.

5. You are prompted to choose the **language** of the installation procedure. Select a language from the list, and press [Enter].

6. You can now select from a menu of **installation options**. Press '2' and [Enter] to update an existing content server.

7. You are prompted to enter the full path to the **installation directory** of the content server to be updated. Specify the installation directory path or accept the default (the detected content server instance on the computer), and press [Enter] to continue.

   If the installer does not detect an existing content server in the specified location, you are prompted to specify the location again.

8. If Microsoft IIS 5.0/6.0 is your web server, complete this step. Otherwise, skip this step and continue with step 10.

   If **file handling caching** is enabled, you are prompted to specify whether it should be disabled. This is recommended so that locked files on your Web site can be updated dynamically without conflict from the web server. Press '1' (yes) or '2' (no), and press [Enter] to continue.

9. If Sun ONE is your web server, complete this step. Otherwise, skip this step and continue with step 10.

   You are prompted to specify the full directory path for the Sun web server to use for the content server. Enter the web server's full directory path, and press [Enter] to continue.

   > **Note:** The directory you specify must contain a subdirectory called 'config' with the files *obj.conf* and *magnus.conf.* The installer will create new *obj.conf* and *magnus.conf* files in the *install* subdirectory of the installation directory. If possible, these files will be installed automatically. The original *obj.conf* and *magnus.conf* files will be renamed *install/obj.conf.orig* and *install/magnus.conf.orig*, respectively.

10. You are prompted to specify what optional components should be enabled with the new content server. These components add functionality to the base content server. You can choose from the following components:

    - ContentFolios
    - Folders_g
    - LinkManager8
    - OracleTextSearch
    - ThreadedDiscussions

    > **Note:** See Appendix C, "Content Server Components" for more information on each of these components.

In addition to these optional components, a number of other components are always installed with the Content Server software. See Appendix C, "Content Server Components" for further details.

> **Note:** The Folders_g component replaces a number of Folders subcomponents automatically at the time of upgrade. You do not need to disable or uninstall the previous version or its subcomponents prior to upgrading to the Folders_g component.

You can toggle a component's installation status by typing its associated number. A currently unselected component is then marked for installation, and vice versa. You use commas to separate multiple components, for example: `1`, `3`. The installation selection of each of these components is then reversed. To unselect all components enter 0.

Type '`f`' (for Finish) when you are done, and press [Enter] to continue.

> **Important:** There are dependencies between Content Server and installed components. If you update your Content Server instance, you should also update all installed components. Similarly, if you update any installed components, you should also update your Content Server instance with the latest patch sets.

> **Note:** The component zip files are all located in the *packages\allplatform* directory of the software distribution package. If you choose not to install a particular component at this point, you can always install it later from this location using the normal methods. See the Content Server administration documentation for more information on installing and enabling components.

11. The installer now performs a number of checks. If there are any errors or warnings, they are reported. Review the installation settings, and then indicate whether the installation should proceed, or abort the installation, or recheck the configuration. Recheck enables you to correct any reported errors before proceeding. When you are ready, choose a menu option and press [Enter] to continue.

12. If you chose to proceed with the installation, all files are copied and the configuration settings made. During that process, a message line shows the percentage of what has been completed, as well as a brief description of the task currently being performed.

> **Note:** This may take some time depending on the number of content items and revision already in the content server.

> **Note:** If you upgraded from a Content Server release prior to with Verity 4.5.1, then the Verity search engine will continue to work after the upgrade to release. If you want, you can switch to database searching and indexing (see "Migrating From Verity to Database Searching/Indexing" on page 6-7). Please note that Content Server does not support Verity 2.7.

When upgrading from a Content Server 7.x version, make sure that the CLASSPATH and JAVA_OPTIONS variables are commented out of the *[CS-Install]/bin/intradoc.cfg* file. To comment out a variable, precede it with a # sign. For example:

```
#CLASSPATH=$COMPUTEDCLASSPATH;$SHAREDDIR/classes/ojdbc14.jar
```

Also, when upgrading from a previous version using Verity as the search engine, make sure that the following variable is set (as shown, in all caps) in the *[CS-Install]/config/config.cfg* file:

```
SearchIndexerEngineName=VERITY.VDK.4
```

13. Restart the computer and start the content server.

14. Verify the installation.

6.4 Updating Proxied Servers

If you are updating an existing 10*g*R3 installation that consists of multiple content server instances, you need to update each instance separately.

If you are updating a pre-10*g*R3 master content server, all of its associated proxied servers on the same system are updated automatically as well. This means that no special steps need to be taken to update them.

> **Important:** After upgrading proxied servers, make sure that you rebuild the static portal page on these servers using the Web Layout Editor.

If you are updating from Content Server 7.5.2 with SQL Server as the database, you need to make some changes to the proxied server(s) when upgrading to the jtds driver for release 10*g*R3. If you are using the jdbc driver that was included in the 7.5.2 media and wish to upgrade, you must perform the following steps for proxied servers after updating the master:

1. Change the following configuration settings in *[Proxy-Install]/config/config.cfg* (see your master's *config/config.cfg* as a sample):

   - JAVA_CLASSPATH_defaultjdbc

   - JdbcDriver

   - JdbcConnectionString

   Example:

```
JAVA_CLASSPATH_defaultjdbc=$SharedDir/classes/jtds-1.2.jar
JdbcDriver=net.sourceforge.jtds.jdbc.Driver
JdbcConnectionString=jdbc:jtds:sqlserver://dbase11:1433/sql19
```

Or, if an explicit path is required, add the following in *[Proxy-Install]*/*bin/ intradoc.cfg* (see your master's *bin/intradoc.cfg* as a sample):

```
JAVA_CLASSPATH_defaultjdbc=[My_Path_to_Driver]/jtds-1.2.jar
```

See "JDBC Drivers and Settings" on page 3-13 for more information about JDBC drivers for SQL Server.

2. Publish static files on the proxied server(s):

   a. Log into the content server as an administrator.

   b. Open the Administrator tray or top menu.

   c. In the **Actions** menu, choose **Publish static layout files**.

6.5 Migrating From Verity to Database Searching/Indexing

If you upgraded from an earlier Content Server release with Verity 4.5.1, then the Verity search engine will continue to work in Content Server 10*g*R3. If you want to, you can easily migrate to database searching and indexing.

Enabling Metadata and Full-Text Searching and Indexing

See Appendix D, "Setting Up Database Search and Indexing" for information about setting up the database for both metadata and full-text searching and indexing.

Enabling Metadata-Only Searching and Indexing

See Appendix D, "Setting Up Database Search and Indexing" for information about setting up the database for metadata-only searching and indexing.

Considerations

Please note the following important considerations:

- Content Server does not support Verity 2.7.

- If you are using the database for full-text searching, its size will increase significantly as a copy of each content item is added to the database for full-text indexing. It is therefore important that you resize your database accordingly. If you did not set up your database to resize automatically, make sure that you give the database sufficient room to grow in size.

7

Starting and Stopping Content Server

This section covers the following topics:

7.1 Starting Content Server

You can start a content server in various ways:

- Startup Options

- Admin Server

- Command Line

7.1.1 Startup Options

There are two options in Microsoft Windows to start Content Server:

- **Automatically starting Content Server as a service**: If Content Server runs as a Windows service, the content server software can start automatically when Windows starts. This enables you to launch a content server instance without logging into Windows.

- **Manually starting Content Server as an application**: You can also start Content Server manually by using the Windows Start menu. From the **Start** menu, select **Programs**, **Content Server**-*[Instance Name]*, and then **Content Server**.

You initially make the choice between starting Content Server automatically (as a service) or manually (as an application) when you install the Content Server software. Regardless of what you choose, a service called IDC Content Service *[Server Name]* is set up for each Content Server instance. Depending on what you chose during setup, its startup type is set to either 'Automatic' or 'Manual'. If you want to change this later, you need to change the startup type by choosing **Start**, then **Settings**, then **Control Panel**, then **Administrative Tools**, and then **Services**.

> **Note:** Another service is always set up in addition to the service called *'IDC Content Service [Server Name]'*. This second service is called 'IDC Content Admin Service', and it enables you to administer a content server remotely using HTML pages.

7.1.2 Admin Server

If the IDC Content Admin Service is running, you can also start a content server remotely from within the Content Server software:

1. Make sure you are logged in with sufficient administrator privileges.

2. Go to the Administration page and click **Admin Server**.

3. All available servers are listed. To start a content server, click its right triangle symbol. (If this symbol is grayed out, it means the server is already running.)

> **Note:** You need to have the 'sysmanager' role to access a content server through Admin Server.

7.1.3 Command Line

You can also start a content server and admin server from the command line using the Launcher, if required with execution flags (parameters). This may be useful for tracing or troubleshooting purposes.

> **Note:** The Launcher is a native C++ application that is provided with Content Server. It allows a Java program to start as a Windows service. For more information about the Launcher and its usage (including the available executable flags or parameters), refer to the *Idc Command Reference Guide*.

To start a content server or admin server from the command line using the Launcher, complete the following steps:

1. Open a command-line window (console), and go the following directory:

   ```
   [CS-Install]\bin\
   ```

2. Start the following executable file to start the content server:

   ```
   IdcServer.exe
   ```

   Start the following executable file to start the admin server:

   ```
   IdcAdmin.exe
   ```

   The content server or admin server will start. The console remains open and shows status information. If the instance was already running, an error message is displayed and the console window remains open.

   You can use the *intradoc.cfg* configuration file in the same directory as *IdcServer.exe* or *IdcAdmin.exe* to control the way the content server or admin server is started. For more information, refer to the *Idc Command Reference Guide*.

> **Tip:** If you want debug information to be displayed in the console, start the content server or admin server executable with the following executable flags (parameters): `-console -debug.`

7.2 Stopping Content Server

If Content Server is running as a **Windows service**, you can stop the service by choosing **Start**, then **Settings**, then **Control Panel**, then **Administrative Tools**, and then **Services**. Select the appropriate service, right-click, and choose **Stop** from the popup menu.

If Content Server is running as an **application**, you can stop the server by simply closing the Content Server window on the server.

Admin Server

If the IDC Content Admin Service is running, you can also stop a content server remotely from within the Content Server software:

1. Make sure you are logged in with sufficient administrator privileges.

2. Go to the Administration page and click **Admin Server**.

3. All available servers are listed. To stop a content server, click its square black symbol. (If this symbol is grayed out, it means the server is already stopped.)

> **Note:** You need to have the 'sysmanager' role to access a content server through Admin Server.

7.3 Restarting Content Server

If Content Server is running as a **Windows service**, you can restart the service by choosing **Start**, then **Settings**, then **Control Panel**, then **Administrative Tools**, and then **Services**. Select the appropriate service, right-click, and choose **Restart** from the popup menu.

If Content Server is running as an **application**, you can restart (stop and start) the server by simply closing the Content Server window and starting it again (see "Starting Content Server" on page 7-1).

Admin Server

If the IDC Content Admin Service is running, you can also restart a content server remotely from within the Content Server software:

1. Make sure you are logged in with sufficient administrator privileges.

2. Go to the Administration page and click **Admin Server**.

3. All available servers are listed. To restart a content server, click its black curved arrow symbol.

> **Note:** You need to have the 'sysmanager' role to access a content server through Admin Server.

> **Note:** You may need to restart the content server if a new component is enabled or if configuration settings or configuration file entries have been changed.

7.4 Logging On to Content Server

To log on to Content Server, complete the following steps:

1. Start your web browser.

2. Go to the Content Server homepage (portal page). By default, the address is *http://[host_name]/[web_root]*, for example *http://master1/server/*.

3. Click the **Login** link in the navigation menu on the left, and verify that your Content Server system administration login is accepted. The defaults are as follows:

   - User name: sysadmin

   - Password: idc

   > **Important:** It is strongly recommended that you change the administrator password from the default to another value.

A

Setting Up Your Web Server

This appendix explains the steps that need to be performed if you set up your web server manually. It covers the following topics:

- "Setting Up IIS 5.0 (Windows 2000 Server)" on page A-1
- "Setting Up IIS 6.0 (Windows Server 2003)" on page A-5
- "Setting Up Sun and Oracle iPlanet Web Servers" on page A-10
- "Setting Up Apache" on page A-14

Important: This section provides guidelines to set up your web server for use with Content Server. Depending on your specific implementation scenario, security requirements or other conditions, a modified setup or additional configuration steps may be required.

Important: Make sure that you read the pre-installation tasks and considerations in Chapter 3, "Pre-Installation Tasks and Considerations."

A.1 Setting Up IIS 5.0 (Windows 2000 Server)

If you chose to set up IIS 5.0 manually during the installation of the Content Server software, you need to complete the following steps:

- Specifying the Web Server
- Setting Up Password Authentication
- Setting Up Virtual Directories (Aliases)
- Setting Up the ISAPI Authentication Filter
- Specifying the Filter Name and Location

Note: Make sure that you read the pre-installation tasks and considerations in Chapter 3, "Pre-Installation Tasks and Considerations."

A.1.1 Specifying the Web Server

Since you chose to set up IIS 5.0 manually, the Content Server installer did not automatically specify the web server in the content server's configuration files. To do this manually, complete the following steps:

1. Go to the file *[CS-Install]\config\config.cfg* (where *[CS-Install]* is the installation directory of the content server instance), and open this file in WordPad.

2. Make sure the file includes the following entry:

   ```
   WebServer=iis
   ```

   (This entry will be typically be under #*Additional Variables*.)

3. Save the modified configuration file and exit WordPad. (If a warning is displayed about saving the file to a text-only format, click **Yes** to confirm the action.)

A.1.2 Setting Up Password Authentication

To specify how IIS 5.0 verifies the identity of users, complete the following steps:

1. From the Windows **Start** menu, choose **Programs**, then **Administrative Tools**, and then **Internet Services Manager**.

   The Internet Information Services screen is displayed.

2. Expand the tree entry of the content server.

   A number of Web sites and/or virtual servers unfold.

3. Select the **Default Web Site** entry, right-click, and then choose **Properties**.

   The Default Web Site Properties screen is displayed.

4. On the Directory Security tab, click **Edit** in the Anonymous access and authentication control box.

   The Authentication Methods screen is displayed.

5. Set the authentication methods as follows:

   - Anonymous access: selected

   - Basic authentication - (password is sent in clear text): cleared

   If you chose to use NT security during the Content Server installation, make sure the Integrated Windows authentication check box is also selected.

6. Click **OK** twice to return to the main Internet Information Services screen.

7. Exit the application, saving any changes you made.

A.1.3 Setting Up Virtual Directories (Aliases)

You need to set up two virtual directories (aliases) to point to the content server's web-viewable file repository (Web Layout) and the filter plugin directory. To accomplish this, complete the following steps:

1. From the Windows **Start** menu, choose **Programs**, then **Administrative Tools**, and then **Internet Services Manager**.

   The Internet Information Services screen is displayed.

2. Expand the tree entry of the content server.

   A number of Web sites and/or virtual servers unfold.

3. Select the **Default Web Site** option, right-click, and then choose **New**, **Virtual Directory**.

    The Virtual Directory Creation Wizard is started.

    > **Important:**   It is extremely important that you create a *new* virtual directory and not use an existing one. Otherwise security issues may arise.

4. Click **Next** in the welcome screen.

5. Enter the virtual directory alias name (typically the content server's relative web root, for example *server*), and click **Next** to continue.

6. Specify the physical path to the web-viewable file directory of the content server instance (for example, *c:\company\idcm1\weblayout*), and click **Next** to continue.

7. Set the access permissions as follows:

    -   Read: selected

    -   Run scripts: cleared

    -   Execute: cleared

    -   Write: set according to your application's requirements

    -   Browse: set according to your application's requirements

    When you are done, click **Next** to continue.

8. Click **Finish** to complete the wizard.

    You are now back in the main Internet Information Services screen.

9. Right-click the virtual directory that you created in step 5, and then choose **Properties**.

10. On the Documents tab, make sure that the Enable Default Document check box is selected and *portal.htm* is included in the box below. If it is not, click **Add**, type *portal.htm*, and click **Apply**.

11. On the Directory Security tab, click **Edit** in the Anonymous access and authentication control box.

    The Authentication Methods screen is displayed.

12. Make sure the Anonymous access check box is selected.

    If you chose to use NT security during the Content Server installation, make sure the Integrated Windows authentication check box is also selected.

13. Click **OK** twice to return to the main Internet Information Services screen.

14. Right-click the virtual directory that you created in step 5, and then choose **New**, **Virtual Directory**.

    Virtual Directory Creation Wizard is started.

15. Click **Next** in the welcome screen.

16. Enter `idcplg` as the virtual directory alias name and click **Next** to continue.

17. Specify the physical path to the filter plugin directory (for example, *c:\company\idcm1\idcplg*), and click **Next** to continue.

18. Set the access permissions as follows:

   ■ Read: cleared

   ■ Run scripts: selected

   ■ Execute: selected

   ■ Write: cleared

   ■ Browse: cleared

   When you are done, click **Next** to continue.

19. Click **Finish** to complete the wizard.

   You are now back in the main Internet Information Services screen.

20. Make sure the virtual directory that you created in step 5 is expanded. Right-click the newly created 'idcplg' item, and then choose **Properties**.

21. On the Documents tab, verify that the Enable Default Document check box is not selected, and click **Apply**.

22. On the Directory Security tab, click **Edit** in the Anonymous access and authentication control box.

   The Authentication Methods screen is displayed.

23. Make sure the Anonymous access check box is selected.

   If you chose to use NT security during the Content Server installation, make sure the Integrated Windows authentication check box is also selected.

24. Click **OK** twice to return to the main Internet Information Services screen.

25. Exit the application, saving any changes you made.

A.1.4 Setting Up the ISAPI Authentication Filter

To set up the ISAPI authentication filter for IIS 5.0, complete the following steps:

1. From the Windows **Start** menu, choose **Programs**, then **Administrative Tools**, and then **Internet Services Manager**.

   The Internet Information Services screen is displayed.

2. Expand the tree entry of the content server.

   A number of Web sites and/or virtual servers unfold.

3. Select the **Default Web Site** option, right-click, and then click **Properties**.

   The Default Web Site Properties screen is displayed.

4. Open the ISAPI Filters tab.

5. Click **Add**.

6. The Filter Properties dialog is displayed.

7. Enter `Idc Plugin [Instance-Name]` in the Filter Name field, for example *Idc Plugin idcm1*.

8. In the Executable field, specify the name and location of the executable ISAPI filter (for example, *c:\company\idcm1\idcplg\idc_cgi_isapi-idcm1.dll*).

9. Click **OK** twice to return to the main Internet Information Services screen.

10. Exit the application, saving any changes you made.

> **Important:** If Microsoft FrontPage is installed, setting up the ISAPI authentication filter will disable Microsoft FrontPage.

After installation of the Content Server software, all web server plugins and cgi programs are available in the following directories:

- [*CS-Install*]\shared\os\win32\lib

- [*CS-Install*]\shared\os\win32\bin

(where *[CS-Install]* is the installation directory of the content server instance).

A.1.5 Specifying the Filter Name and Location

If you set up IIS 5.0 manually, you need to check the references to the content server web filter in the following configuration files:

- [*CS-Install*]\admin\config\config.cfg

- [*CS-Install*]\config\config.cfg

- [*CS-Install*]\admin\data\servers*[Instance-Name]*\server.hda

(where *[CS-Install]* is the installation directory of the content server instance and *[Instance-Name]* the name of the instance).

HTTP Relative CGI Root

The HTTP relative CGI root is the location of Content Server's web filter. The default location is the *idcplg* subdirectory of the content server instance root directory (for example, *c:\company\idcm1\idcplg*). If you want to use a different directory, you need to make sure each of the configuration files above refers to the correct location (which is a subdirectory of server instance's installation directory):

```
HttpRelativeCgiRoot=/[New_Directory]/
```

CGI File Name

You need to make sure that each of the configuration files above contains the following entry:

```
CgiFileName=idcplg
```

(If the `CgiFileName` entry already exists, modify it to match the line above.)

A.2 Setting Up IIS 6.0 (Windows Server 2003)

If you chose to set up IIS 6.0 manually during the installation of the Content Server software, you need to complete the following steps:

- Specifying the Web Server

- Setting Up Password Authentication

- Setting Up Virtual Directories (Aliases)

- Setting Up the ISAPI Authentication Filter

- Specifying the Filter Name and Location

- Setting Up the Web Service Extension

- Registering MIME Types

> **Note:** Make sure that you read the pre-installation tasks and considerations in Chapter 3, "Pre-Installation Tasks and Considerations."

A.2.1 Specifying the Web Server

Since you chose to set up IIS 6.0 manually, the Content Server installer did not automatically specify the web server in the content server's configuration files. To do this manually, complete the following steps:

1. Go to the file *[CS-Install]\config\config.cfg* (where *[CS-Install]* is the installation directory of the content server instance), and open this file in WordPad.

2. Make sure the file includes the following entry:

   ```
   WebServer=iis
   ```

   (This entry will be typically be under #*Additional Variables*.)

3. Save the modified configuration file and exit WordPad. (If a warning is displayed about saving the file to a text-only format, click **Yes** to confirm the action.)

A.2.2 Setting Up Password Authentication

To specify how IIS 6.0 verifies the identity of users, complete the following steps:

1. From the Windows desktop, choose **Start**, then **Administrative Tools**, and then **Internet Information Services (IIS) Manager**.

   The Internet Information Services (IIS) Manager screen is displayed.

2. Expand the tree entry of the content server.

3. Expand the Web Sites entry.

   A number of Web sites and/or virtual servers unfold.

4. Select the **Default Web Site** entry, right-click, and then choose **Properties**.

   The Default Web Site Properties screen is displayed.

5. On the Directory Security tab, click **Edit** in the Authentication and access control box.

   The Authentication Methods screen is displayed.

6. Set the authentication methods as follows:

   - Enable anonymous access: selected
   - Basic authentication (password is sent in clear text): cleared

   > **Note:** Do not change the user name or password for anonymous access.

   If you chose to use NT security during the Content Server installation, make sure the Integrated Windows authentication check box is also selected.

7. Click **OK** twice to return to the main Internet Information Services screen.

8. Exit the application, saving any changes you made.

A.2.3 Setting Up Virtual Directories (Aliases)

You need to set up two virtual directories (aliases) to point to the content server's web-viewable file repository (Web Layout) and the filter plugin directory. To accomplish this, complete the following steps:

1. From the Windows desktop, choose **Start**, then **Administrative Tools**, and then **Internet Information Services (IIS) Manager**.

    The Internet Information Services (IIS) Manager screen is displayed.

2. Expand the tree entry of the content server.

3. Expand the Web Sites entry.

    A number of Web sites and/or virtual servers unfold.

4. Select the **Default Web Site** option, right-click, and then choose **New**, **Virtual Directory...**.

    The Virtual Directory Creation Wizard is started.

    > **Important:**   It is extremely important that you create a *new* virtual directory and not use an existing one. Otherwise security issues may arise.

5. Click **Next** in the welcome screen.

6. Enter the virtual directory alias name (typically the content server's relative web root, for example *server*), and click **Next** to continue.

7. Specify the physical path to the web-viewable file directory of the content server instance (for example, *c:\company\idcm1\weblayout*), and click **Next** to continue.

8. Set the access permissions as follows:

    - Read: selected
    - Run scripts: cleared
    - Execute: cleared
    - Write: set according to your application's requirements
    - Browse: set according to your application's requirements

    When you are done, click **Next** to continue.

9. Click **Finish** to complete the wizard. You are now back in the main Internet Information Services (IIS) Manager screen.

10. Right-click the virtual directory that you created in step 6, and then choose **Properties**.

11. On the Documents tab, make sure that the Enable default content page check box is selected and *portal.htm* is included in the box below. If it is not, click **Add**, type *portal.htm*, and click **Apply**.

12. On the Directory Security tab, click **Edit** in the Authentication and access control box.

    The Authentication Methods screen is displayed.

13. Make sure the Enable anonymous access check box is selected.

If you chose to use NT security during the Content Server installation, make sure the Integrated Windows authentication check box is also selected.

14. Click **OK** twice to return to the main Internet Information Services screen.

15. Right-click the virtual directory that you created in step 6, and then choose **New**, **Virtual Directory...**.

The Virtual Directory Creation Wizard is started.

16. Click **Next** in the welcome screen.

17. Enter idcplg as the virtual directory alias name and click **Next** to continue.

18. Specify the physical path to the filter plugin directory (for example, *c:\company\idcm1\idcplg*), and click **Next** to continue.

19. Set the access permissions as follows:

- Read: cleared
- Run scripts: selected
- Execute: selected
- Write: cleared
- Browse: cleared

When you are done, click **Next** to continue.

20. Click **Finish** to complete the wizard.

You are now back in the main Internet Information Services (IIS) Manager screen.

21. Make sure the virtual directory that you created in step 6 is expanded. Right-click the newly created 'idcplg' item, and then choose **Properties**.

22. On the Documents tab, verify that the Enable default content page check box is not selected, and click **Apply**.

23. On the Directory Security tab, click **Edit** in the Authentication and access control box.

The Authentication Methods screen is displayed.

24. Make sure the Enable anonymous access check box is selected (do not change the user name or password).

25. Click **OK** twice to return to the main Internet Information Services (IIS) Manager screen.

26. Exit the application, saving any changes you made.

A.2.4 Setting Up the ISAPI Authentication Filter

To set up the ISAPI authentication filter for IIS 6.0, complete the following steps:

1. From the Windows desktop, choose **Start**, **Administrative Tools**, and then **Internet Information Services (IIS) Manager**.

The Internet Information Services (IIS) Manager screen is displayed.

2. Expand the tree entry of the content server.

3. Expand the Web Sites entry.

A number of Web sites and/or virtual servers unfold.

4. Select the **Default Web Site** option, right-click, and then click **Properties**.

   The Default Web Site Properties screen is displayed.

5. Open the ISAPI Filters tab.

6. Click **Add**.

7. The Add/Edit Filter Properties dialog is displayed.

8. Enter `Idc Plugin [Instance-Name]` in the Filter Name field, for example *Idc Plugin idcm1*.

9. In the Executable field, specify the name and location of the executable ISAPI filter (for example, *c:\company\idcm1\idcplg\idc_cgi_isapi-idcm1.dll*).

10. Click **OK** twice to return to the main Internet Information Services (IIS) Manager screen.

11. Exit the application, saving any changes you made.

> **Important:** If Microsoft FrontPage is installed, setting up the ISAPI authentication filter will disable Microsoft FrontPage.

After installation of the Content Server software, all web server plugins and cgi programs are available in the following directories:

- [*CS-Install*]\shared\os\win32\lib

- [*CS-Install*]\shared\os\win32\bin

(where *[CS-Install]* is the installation directory of the content server instance).

A.2.5 Specifying the Filter Name and Location

If you set up IIS 6.0 manually, you need to check the references to the content server web filter in the following configuration files:

- [*CS-Install*]\admin\config\config.cfg

- [CS-*Install*]\config\config.cfg

- [CS-*Install*]\admin\data\servers\[*Instance-Name*]\server.hda

(where *[CS-Install]* is the installation directory of the content server instance and *[Instance-Name]* the name of the instance).

HTTP Relative CGI Root

The HTTP relative CGI root is the location of Content Server's web filter. The default location is the *idcplg* subdirectory of the content server instance root directory (for example, *c:\company\idcm1\idcplg*). If you want to use a different directory, you need to make sure each of the configuration files above refers to the correct location (which is a subdirectory of server instance's installation directory):

```
HttpRelativeCgiRoot=/[New_Directory]/
```

CGI File Name

You need to make sure that each of the configuration files above contains the following entry:

```
CgiFileName=idcplg
```

(If the `CgiFileName` entry already exists, modify it to match the line above.)

A.2.6 Setting Up the Web Service Extension

If you set up IIS 6.0 manually, you need to set up the web service extension:

1. From the Windows desktop, choose **Start**, then **Administrative Tools**, and then **Internet Information Services (IIS) Manager**.

   The Internet Information Services (IIS) Manager screen is displayed.

2. Expand the tree entry of the content server.

3. Select the Web Service Extensions link.

4. Click on **Add a new Web service extension...**.

5. Provide an extension name, for example *Idc Plugin idcm1*.

6. Click the **Add** button to add the required file, for example *[CS-Install]\idcplg\idc_cgi_isapi_idcm1.dll (*where *[CS-Install]* is the installation directory of the content server instance).

7. Make sure that you select the "Set extension status to Allowed" check box.

A.2.7 Registering MIME Types

For security reasons, IIS 6.0 will not serve a file if its file extension is not registered as a MIME type for the Web site. Depending on the file types handled by your content server, you may need to register their MIME types with IIS, so the web server will serve the associated file types to the client browsers. For further details, refer to Chapter 5, "Post-Installation Tasks and Considerations."

A.3 Setting Up Sun and Oracle iPlanet Web Servers

If you chose to set up the Sun or iPlanet web servers manually during the installation of the Content Server software, you need to complete the following steps:

- Adding an Additional Document Directory
- Specifying the CGI Directory
- Modifying the <host-name>-obj.conf File
- Modifying the magnus.conf File
- Specifying the Filter Name and Location
- Setting Up Sun Web Server for Proxy Instances (if applicable)

> **Note:** Make sure that you read the pre-installation tasks and considerations in chapter Chapter 3, "Pre-Installation Tasks and Considerations."

A.3.1 Adding an Additional Document Directory

The web server needs to know where the content server's web-viewable file repository (*weblayout* directory) is located. To accomplish this, complete the following steps:

1. Launch the Administer Web Server utility.

2. Enter the user name and password.

3. Select your server, and then click **Manage**.

4. Click **Class Manager** in the top right-hand corner of the page.

5. Open the **Content Mgmt** tab.

6. Click the **Additional Document Directories** link on the left side of the page.

7. Enter *oracle* as the URL prefix.

8. Enter *[CS-Install]*/`weblayout` as the directory to map to (where *[CS-Install]* is the installation directory of the content server instance), for example:

   ```
   c:/oracle/ucm/contentserver/weblayout
   ```

9. Click **OK** when you are done.

A.3.2 Specifying the CGI Directory

The web server needs to know where the content server's CGI directory is located. To accomplish this, complete the following steps:

1. Launch the Administer Web Server utility.

2. Enter the user name and password.

3. Select your server, and then click **Manage**.

4. Click **Class Manager** in the top right-hand corner of the page.

5. Open the **Programs** tab.

6. Click the **CGI Directory** link on the left side of the page.

7. Enter `idcplg` as the URL prefix.

8. Enter *[CS-Install]*/`idcplg` as the CGI directory (where *[CS-Install]* is the installation path of the content server instance), for example:

   ```
   c:/oracle/ucm/contentserver/idcplg
   ```

9. Click **OK** when you are done.

A.3.3 Modifying the *<host-name>*-obj.conf File

You need to modify the *<host-name>*-obj.conf file of the Sun web server to include two new entries:

1. Go to the Sun web server software directory, and open the *https-[host-name]\config* subdirectory (where *[host-name]* is the name of the system on which the software is installed), for example:

   ```
   c:\iplanet\servers\https-server7\config
   ```

2. Open the file *<host-name>*-obj.conf in a text editor.

3. Add the following 'ppath' object to the *<host-name>*-obj.conf file:

   ```
   <Object path="[Weblayout_Dir]/*">
   NameTrans fn="idcNameTrans"
   PathCheck fn="idcPathCheck"
   Service fn="idcService"
   </Object>
   ```

   (*[Weblayout_Dir]* is the full path to the web-viewable file repository, for example c:*/oracle/ucm/contentserver/weblayout*.)

> **Note:** Enter the Object entry above on multiple lines, as shown.

4. Inside the <Object name="default"> section, add the following line:

```
NameTrans fn="pfx2dir" from="/[Relative_Web_Root]" dir="[Weblayout_Dir]"
```

(*[Relative_Web_Root]* is the relative web root of the content server instance, and *[Weblayout_Dir]* is the full path to the web-viewable file repository.) Example:

```
NameTrans fn="pfx2dir" from="/oracle"
dir="c:/oracle/ucm/contentserver/weblayout"
```

> **Important:** Enter the NameTrans entry above on a singe line and not on multiple lines as shown (add a space instead of a line break).

5. Apply the changes that you just made to the *<host-name>*-obj.conf file on the web server's administration page.

6. Stop and restart the web server.

A.3.4 Modifying the magnus.conf File

You need to configure the *magnus.conf* file of the Sun web server to include two new entries:

1. Go to the Sun web server software directory, and open the *https-[host_name]\config* subdirectory (where *[host_name]* is the name of the system on which the software is installed), for example:

```
c:\iplanet\servers\https-server7\config
```

2. Open the file *magnus.conf* in a text editor.

   Add the following entries after the last 'Init fn' entry:

```
Init fn="load-modules"
funcs="idcInit,idcNameTrans,idcPathCheck,idcService"
shlib="[CS-Install]/shared/os/win32/lib/IdcNSAuth.dll"
Init fn="idcInit" idocdb="[Inst_Dir]/data/users/userdb.txt"
```

(*[CS-Install]* is the full path to the installation directory of the content server instance.)

> **Important:** Enter each of the Init entries above on a singe line and not on multiple lines as shown (add a space instead of a line break).

3. Apply the changes that you just made to the *magnus.conf* file on the web server's administration page.

4. Stop and restart the web server.

A.3.5 Specifying the Filter Name and Location

You need to check the name and location of the content server web filter. This file is referenced in the following configuration files:

- [*CS-Install*]\admin\config\config.cfg

- [*CS-Install*]\config\config.cfg

- [*CS-Install*]\admin\data\servers*[Instance-Name]*\server.hda

(where *[CS-Install]* is the installation directory of the content server instance and *[Instance-Name]* its name).

HTTP Relative CGI Root

The HTTP relative CGI root is the location of Content Server's web filter. The default location is the *idcplg* subdirectory of the content server instance root directory (for example, *c:\oracle\ucm\contentserver\idcplg*). If you want to use a different directory, you need to make sure each of the configuration files above refers to the correct location (which is a subdirectory of server instance's installation directory):

```
HttpRelativeCgiRoot=/[New_Directory]/
```

CGI File Name

You need to make sure that each of the configuration files above contains the following entry:

```
CgiFileName=idcplg
```

(If the `CgiFileName` entry already exists, modify it to match the line above.)

A.3.6 Setting Up Sun Web Server for Proxy Instances

If you installed the content server as a proxy instance (on the same computer as the master and the web server), then you also need to perform the following steps:

1. Add an additional document directory to the web server (using Sun's Administer Web Server utility; see "Adding an Additional Document Directory" on page A-10). For example, if the relative web root of the proxy instance is 'UCM-2', then you enter `UCM-2` as the URL prefix and map it to your proxy's *weblayout* directory.

2. Add an additional path object in the web server's *obj.conf* (see "Modifying the <host-name>-obj.conf File" on page A-11), for example:

```
<Object path="[Proxy_Weblayout_Dir]/*">
NameTrans fn="idcNameTrans"
PathCheck fn="idcPathCheck"
Service fn="idcService"
</Object>
```

(*[Proxy_Weblayout_Dir]* is the full path to the web-viewable file repository of the proxy server, for example c:/*oracle/ucm/contentserver/idcm1p1/weblayout*.)

> **Note:** Enter the Object entry above on multiple lines, as shown.

3. Inside the <Object name="default"> section of *obj.conf* (see "Modifying the <host-name>-obj.conf File" on page A-11), add the following entry for the proxy instance, for example:

```
NameTrans fn="pfx2dir" from="/[Proxy_Rel_Web_Root]" dir="[Proxy_Weblayout_Dir]"
```

([Proxy_Rel_Web_Root] is the relative web root of the proxy instance, and *[Proxy_ Weblayout_Dir]* is the full path to the web-viewable file repository of the proxy instance.) Example:

```
NameTrans fn="pfx2dir" from="/UCM_2"
dir="c:/oracle/ucm/contentserver/idcm1p1/weblayout"
```

> **Important:**   Enter the NameTrans entry above on a singe line and not on multiple lines as shown (add a space instead of a line break).

4. Apply the changes that you just made to the *obj.conf* file on the web server's administration page.

5. Stop and restart the web server.

A.4 Setting Up Apache

Since Apache cannot be configured automatically by the Content Server installer, you need to do it manually. This consists of the following :

- Configuring Apache for Master Instances
- Configuring Apache for Proxied Instances
- Enabling Debug on Apache
- Log Dump File
- Turning Off Canonical Names

> **Note:**   Make sure that you read the pre-installation tasks and considerations in Chapter 3, "Pre-Installation Tasks and Considerations."

A.4.1 Configuring Apache for Master Instances

To configure Apache for master instances, complete the following steps:

1. Choose a master content server (that is, one content server on the computer that is not a proxied content server), and add the following configuration entry to the bottom of the *httpd.conf* file (or at least below the 'clearmodulelist' line):

> **Important:**   For Apache 2.0.59 specify IdcApache2Auth.dll.
> For Apache 2.2.4 specify IdcApache22Auth.dll.

- **Windows:**

  ```
  LoadModule IdcApacheAuth [Webserver_Filters_Path] /IdcApache2Auth.dll
  ```

> **Note:**   The path to the web server filters is usually *[Root_Dir_For_ Master]\shared\os\win32\lib*. *[Master_Instance]* is usually the instance name of the master content server (IDC_NAME parameter in *config.cfg*). The path to the user data directory is usually *[Root_Dir_ For_Master]\data\users*.

For example:

```
LoadModule IdcApacheAuth
C:/oracle/ucm/contentserver/shared/os/win32/lib/IdcApache2Auth.dll
```

(Please note that the entry above is on a single line.)

2. For each master content server (that is, for each content server on the computer that is not a proxied content server), add the following configuration entry to the bottom of the *httpd.conf* file (or at least below the 'clearmodulelist' line)

   ■ **Windows**:

   ```
   IdcUserDB [Master_Instance] "[User_Data_Dir_Path]/userdb.txt"
   ```

   For example:

   ```
   IdcUserDB UCM "C:/oracle/ucm/contentserver/data/users/userdb.txt"
   ```

3. Add the following entries to set up the alias to the master server *weblayout* directory and have its security controlled by the filter.

   ```
   Alias /[Rel._URL_To_Master] "[Path_To_Master_Webl.]"
   <Location /[Rel._URL_To_Master]>
       Order allow,deny
       Allow from all
       DirectoryIndex portal.htm
       IdcSecurity [Master_Instance]
   </Location>
   ```

   For example:

   ```
   Alias /idcm1 "C:/oracle/ucm/contentserver/weblayout"
   <Location /idcm1>
       Order allow,deny
       Allow from all
       DirectoryIndex portal.htm
       IdcSecurity idcm1
   </Location>
   ```

   > **Note:** The path to the web layout of the master content server is usually *[Root_Dir_For_Master]\weblayout*, but it may be relocated to another disk drive. The relative URL to the master content server should be specified without its trailing slash. *[Master_Instance]* is usually the instance name of the master content server (IDC_NAME parameter in *config.cfg*) and should match the name used for the IdcUserDB entry.

A.4.2 Configuring Apache for Proxied Instances

For each proxied server, add an alias and security entry for the *weblayout* directory to the *httpd.conf* file:

```
Alias /[Rel._URL_To_Prox.] "[Path_To_Prox._Weybl.]"
<Location /[Rel._URL_To_Prox.]>
    Order allow,deny
    Allow from all
    DirectoryIndex portal.htm
    IdcSecurity [Master_Instance]
</Location>
```

For example:

```
Alias /UCM_2 "C:/oracle/ucm/contentserver/idcm1p1/weblayout"
<Location /UCM_2>
    Order allow,deny
    Allow from all
    DirectoryIndex portal.htm
    IdcSecurity UCM
</Location>
```

> **Note:** The path to the web layout of the master content server is usually [*Root_Dir_For_Master*]weblayout, but it may be relocated to another disk drive. The relative URL to the master content server should be specified without its trailing slash. *[Master_Instance]* is usually the instance name of the master content server (IDC_NAME parameter in *config.cfg*) and should match the name used for the IdcUserDB entry.

A.4.3 Enabling Debug on Apache

To enable debug on Apache, complete the following steps:

1. Log into the content server as an administrator.

2. Open the Administration page.

3. Click on the **Filter Administration** link. (You may need to scroll down.)

   The Configure Web Server Filter page is displayed.

4. Under Logging Options, make sure that the CGI_RECEIVE_DUMP and CGI_SEND_DUMP options are both selected.

5. Click the **Update** button in the Logging Options section.

A.4.4 Log Dump File

The log dump will go to the file [*CS-Install*]/data/users/authfilter.log, where [*CS-Install*] is the installation directory of the content server instance.

A.4.5 Turning Off Canonical Names

Your content servers may use an IP address or an address that is different from the physical server they are running on (i.e., the *HttpServerAddress* variable is defined in Content Server's *config.cfg* file). If that is the case, it is a good idea to turn off canonical names. With this setting turned on, whenever Apache needs to construct a self-referencing URL (i.e., a URL that refers back to the server the response is coming from), it will use ServerName and Port to form a canonical name. With this setting turned off, Apache will use the hostname:port that the client supplied (if possible). This eliminates double login prompts.

To turn canonical names off, make sure the *httpd.conf* file includes the following line:

```
UseCanonicalName Off
```

(Please note the default setting is 'On'.)

A.4.6 Indexing Portal Page

To make the portal.htm page of Content Server the index when using Apache as your web server, set `ApacheConfLocationSectionExtraText=DirectoryIndex portal.htm` in the Content Server config.cfg file using a standard text editor. Please note the space between "DirectoryIndex portal.htm" when setting the variable. The config.cfg file is located in the `<install_dir>/<instance_dir>/config` directory.

B

Setting Up Your Database

The Content Server software installer can set up some databases automatically for use with your content server, although you may choose to do this manually. This appendix explains the steps that need to be performed to set up your database manually. It covers the following topics:

- "Database Scripts" on page B-1
- "Setting Up SQL Server" on page B-2
- "Setting Up Oracle" on page B-6
- "Setting Up Sybase" on page B-13
- "Setting Up DB2" on page B-16

> **Important:** This section provides guidelines to set up your database for use with Content Server. Depending on your specific implementation scenario, security requirements or other conditions, a modified setup or additional configuration steps may be required.

> **Note:** Make sure that you read the pre-installation tasks and considerations in Chapter 3, "Pre-Installation Tasks and Considerations."

B.1 Database Scripts

The Content Server software is shipped with a number of scripts for each supported database which enable you to create and populate the tablespaces manually.

Script Locations

Before the Content Server installation, these scripts are available in each Content Server software distribution package:

`\UCM\ContentServer\database\[DB_Name]`

After the Content Server installation, the scripts are also available at:

`[CS-Install]\database\[DB_Name]`

(where *[CS-Install]* is the installation directory of the content server instance).

Unicode Text Fields

As an alternative to using UTF-8 database tables, you can use Unicode text fields with the content server if the database is not Oracle.

If you want to use Unicode text fields in your database tables, make sure that you use the database scripts in the *unicode* subdirectory of the above locations. If you use the Unicode scripts, the 'nvarchar' data type is used for the database columns created for the content server rather than the 'varchar' data type.

Like UTF-8 text fields, unicode text fields give you more flexibility as the database can handle virtually any language. Note that it doubles the size of the database, since every character is represented as two bytes rather than one.

Choosing Unicode encoding does not affect the language encoding, or charset, of the database. It only affects the data types of the database columns created for the content server ('nvarchar' rather than 'varchar'). Also, the data encoding for the Content Server database does not apply to the entire enterprise database, but only to Content Server's reserved tablespace within that database.

Script Order

When running the scripts, always make sure that you run them in the following order:

- intradoc.sql
- default.sql
- formats.sql
- format_defaults.sql
- users.sql
- workflow.sql

Depending on the database, there may also be an *all.sql* script, which enables you to run all the above scripts in a single operation and in the correct order.

B.2 Setting Up SQL Server

If you are setting up SQL Server 2008 or you chose to set up SQL Server 2000 or 2005 manually during the installation of the Content Server software, you need to complete the following:

- Creating the Content Server Database
- Creating the Database Tables
- Configuring the JDBC Settings
- Specifying the Classpath
- Rebuilding the Content Server Portal Page
- Restarting the Server(s)

> **Note:** If you want to set up SQL Server for full-text database searching and indexing, refer to Appendix D, "Setting Up Database Search and Indexing."

B.2.1 Creating the Content Server Database

If you did not already create the Content Server database in SQL Server, you need to do so by completing the following steps:

1. From the Windows Start menu, navigate to the Microsoft SQL Server application group and start **Enterprise Manager** (for SQL Server 2000 and 2005) or **SQL Server Management Studio** (for SQL Server 2008).

   The SQL Server management console is displayed.

2. In the tree view on the left, select the server on which the Content Server database will reside (you may need to expand one or more tree branches).

3. Select the Databases entry, then right-click and choose **New Database...** from the popup menu.

   The Database Properties dialog is displayed.

4. On the General tab, specify a meaningful name for the new database.

5. On the Data Files tab, you can specify the database file name and location. Also, make sure that you set the initial file size of 100 MB and that you allow the database to grow automatically by 10 percent.

6. On the Transaction Logs tab, you can specify the log file name and location. Also, make sure that you set the initial file size of 25 MB and that you allow the log file to grow automatically by 10 percent.

7. By default, Content Server 10*g*R3 uses SQL Server authentication to access the SQL Server database. If you want to use Windows NT authentication rather than SQL Server authentication, you must make sure that the default authentication method for SQL Server is set correctly:

   a. Launch the SQL Server Enterprise Manager.

   b. Select the database server.

   c. Right-click, and choose **Properties** from the pop-up menu.

   d. Open the Security tab.

   e. In the Security area, make sure that the authentication is set to 'SQL Server and Windows'. (This is not the default value.)

8. Exit the SQL Server management console.

B.2.2 Creating the Database Tables

You need to create the database tables in the Content Server database. This is accomplished by running a series of SQL scripts that are shipped with the Content Server software. If the content server tables already exist, they will be dropped and re-created.

To create the SQL Server database tables, complete the following steps:

1. From the Windows Start menu, choose **Programs**, then **Microsoft SQL Server**, and then **Enterprise Manager**.

   The SQL Server Enterprise Manager console is displayed.

2. In the tree view on the left, select the server on which the Content Server database resides (you may need to expand one or more tree branches).

3. From the Tools menu, choose SQL Query Analyzer.

The SQL Query Analyzer window is displayed.

4. From the drop-down list in the toolbar, select the Content Server database.

5. Choose **File**, then **Open**, and browse to the location of the scripts for SQL Server:

   SQL Server 2000: If you are setting up SQL Server *before* installing the Content Server software, you can find the script files in the following location on the Content Server software distribution media:

   - For non-Unicode text fields (varchar) in the database tables: *\UCM\ContentServer\database\mssql2000*

   - For Unicode text fields (nvarchar) in the database tables: *\UCM\ContentServer\database\mssql2000\unicode*

   If you are setting up SQL Server 2000 *after* installing the Content Server software, the script files are also available in the *[CS-Install]\database\mssql2000* directory and its *unicode* subdirectory.

   SQL Server 2005 or SQL Server 2008: If you are setting up SQL Server *before* installing the Content Server software, you can find the script files in the following location on the Content Server software distribution media:

   - For non-Unicode text fields (varchar) in the database tables: *\UCM\ContentServer\database\mssql*

   - For Unicode text fields (nvarchar) in the database tables: *\UCM\ContentServer\database\mssql\unicode*

   If you are setting up SQL Server 2005 or SQL Server 2008 *after* installing the Content Server software, the script files are also available in the *[CS-Install]\database\mssql* directory and its *unicode* subdirectory.

6. Open each of the following scripts (in the order provided) and choose **Query**, then **Execute** (or press F5) to run it:

   - intradoc.sql

   - default.sql

   - formats.sql

   - format_defaults.sql

   - users.sql

   - workflow.sql

   Note: You may get error messages because these procedures try to drop tables that do not yet exist in an initial install. You may safely ignore these error messages.

   ---

7. Exit the SQL Query Analyzer.

8. Exit the SQL Server management console.

B.2.3 Configuring the JDBC Settings

For the content server to communicate with SQL Server successfully, you need to configure the JDBC settings in Content Server. To do this, complete the following steps:

> **Note:** This procedure assumes that you will use the jTDS driver. If you are using a different driver, then the driver name and connection string will be different.

1. From the Windows Start menu, select **Programs**, then **Content Server-[*Instance Name]*, **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Database tab.

3. Select the following options.

   - Use Java Database Connectivity

   - JTDS JDBC Driver

4. Specify the following as the JDBC driver name:

   ```
   net.sourceforge.jtds.jdbc.Driver
   ```

5. Specify the JDBC connection string as follows, depending on the SQL Server authentication method you want to use:

   SQL Server authentication:

   ```
   jdbc:jtds:sqlserver://[DB_Server]:[Port_No]/[DB_Name]
   ```

   Windows authentication:

   ```
   jdbc:jtds:sqlserver://[DB_Server]:[Port_No]/ [DB_Name]:domain=[Domain_Name]
   ```

   where *[DB_Server]* is the name of the database server, *[Port_No]* is the port number (usually 1433), *[DB_Name]* is the Content Server database name, and *[Domain_ Name]* the name of the Windows network domain. For example (for SQL Server authentication):

   ```
   jdbc:jtds:sqlserver://csdb:1433/oracle
   ```

6. Make sure that the authentication method is set correctly in SQL Server:

   a. Launch the SQL Server Enterprise Manager.

   b. Select the database server.

   c. Right-click, and choose **Properties** from the pop-up menu.

   d. Open the Security tab.

   e. In the Security area, select 'SQL Server and Windows' for SQL Server authentication, or 'Windows only' for Windows authentication.

7. Also provide the JDBC user name and password as required. These are the user name and password used to connect to the SQL Server database.

8. Click **OK** to save the changes and exit the System Properties utility.

B.2.4 Specifying the Classpath

For the content server to communicate with SQL Server successfully, you need to provide a reference to the JDBC driver file that is used with the database. To do this, complete the following steps:

1. From the Windows Start menu, select **Programs**, then **Content Server**-*[Instance Name]*, **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Paths tab.

3. Specify the following as the classpath:

   ```
   JAVA_CLASSPATH_defaultjdbc;$SharedDir/classes/jtds.jar
   ```

4. Click **OK** to save the changes and exit the System Properties utility.

B.2.5 Rebuilding the Content Server Portal Page

You need to rebuild the content server portal page. To do this, complete the following steps:

1. From the Windows Start menu, choose **Programs**, then **Content Server**-*[Instance Name]*, and then **Weblayout Editor**.

2. Choose **Update Portal** from the Options menu.

3. Click **OK**.

B.2.6 Restarting the Server(s)

As the final step, you need to (re)start the content server. If the database is installed on a proxied server, make sure that you restart the content servers in the following order:

1. Restart the proxied server that the SQL Server database was installed on.

2. Restart the master server.

3. Restart the proxied server again.

The database is now ready for use with Content Server.

B.3 Setting Up Oracle

If you chose to set up an Oracle database manually during the installation of the Content Server software, you need to complete the following steps:

- Creating the Content Server Database
- Creating the Database Tables
- Configuring the JDBC Settings
- Specifying the Classpath
- Rebuilding the Content Server Portal Page
- Restarting the Server(s)
- Setting Up the Oracle OCI Driver (Oracle9i) (if required)
- Setting Up the Oracle OCI Driver (Oracle 10g) (if required)

> **Note:** If you want to set up Oracle for full-text database searching and indexing, refer to Chapter D, "Setting Up Database Search and Indexing."

B.3.1 Creating the Content Server Database

If you did not already create the Content Server database in Oracle, you need to do so. Refer to Chapter 3, "Pre-Installation Tasks and Considerations" for further guidelines and considerations.

B.3.2 Creating the Database Tables

You need to create the database tables in the Content Server database. This is accomplished by running a series of SQL scripts that are shipped with the Content Server software. If the content server tables already exist, they will be dropped and re-created.

To create the Oracle database tables, complete the following steps:

1. Change your working directory to the following:

    ■   *[CS-Install]*\database\oracle

    (where *[CS-Install]* is the installation directory of the content server instance).

2. Start SQL*Plus and log in to the database using the Oracle user name and password for the content server.

3. Enter the following command at the SQL prompt: @all.sql.

    > **Note:**   You may get error messages because this procedure tries to delete tables that do not yet exist in an initial install. You may safely ignore these error messages.

4. When the script has completed, exit SQL*Plus.

B.3.3 Configuring the JDBC Settings

For the content server to communicate with Oracle successfully, you need to configure the JDBC settings in Content Server. To do this, complete the following steps:

> **Note:**   This procedure assumes you will use the Oracle Thin JDBC driver. If you want to use the Oracle OCI driver instead, refer to "Setting Up the Oracle OCI Driver (Oracle9i)" on page B-9 or "Setting Up the Oracle OCI Driver (Oracle 10g)" on page B-11 for further information.

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

    The System Properties applet is started.

2. Open the Database tab.

3. Select the following options:

    ■   Use Java Database Connectivity

    ■   Oracle Thin JDBC Driver

4. Modify the JDBC connection string to suit your specific application. Use the following string format:

    jdbc:oracle:thin:@*[DB_Host_Name]*:*[DB_Server_Port]*/*[DB_Name]*

where *[DB_Host_Name]* is the host name of the Oracle server, *[DB_Server_Port]* is the port number (usually 1521), and *[CS_Name]* is the database instance name, for example:

```
jdbc:oracle:thin:@csoracle:1521/oracle
```

5. Also provide the JDBC user name and password as required. These are the user name and password used to connect to the Oracle database.

> **Note:** The JDBC user name and password should be same as the one used to create the Oracle tables. If the JDBC user does not have access privileges to the tables, the content server will fail to start.

6. Click **OK** to save the changes and exit the System Properties utility.

B.3.4 Specifying the Classpath

For the content server to communicate with Oracle successfully, you need to provide a reference to the JDBC driver file that is used with the database. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Paths tab.

3. Specify the following as the classpath:

   ```
   JAVA_CLASSPATH_defaultjdbc;$SharedDir/classes/ojdbc14.jar
   ```

4. Click **OK** to save the changes and exit the System Properties utility.

B.3.5 Rebuilding the Content Server Portal Page

You need to rebuild the content server portal page. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Choose **Update Portal** from the Options menu.

3. Click **OK**.

B.3.6 Restarting the Server(s)

As the final step, you need to (re)start the content server. If the database is installed on a proxied server, make sure that you restart the content servers in the following order:

1. Restart the proxied server that the Oracle database was installed on.

2. Restart the master server.

3. Restart the proxied server again.

Oracle is now ready for use with Content Server.

B.3.7 Setting Up the Oracle OCI Driver (Oracle9i)

Instead of the JDBC thin client for communication with Oracle9*i*, you may also choose to use Oracle's OCI driver. If you did not select this driver during the Content Server installation, you need to set it up manually:

- Installing the Oracle Client
- Copying the Oracle JDBC Driver
- Editing the tnsnames.ora File
- Editing the intradoc.cfg File
- Copying the Oracle Shared Library File
- Changing the Database Settings

B.3.7.1 Installing the Oracle Client

To install the Oracle Client, complete the following steps:

1. Install the Oracle Client on the computer running Content Server. This will install Net9 and OCI libraries on the content server. The Oracle Client is included on the Oracle software distribution media.

2. Configure the Oracle Client so that it can successfully communicate with the Oracle server. Place the dll files into your *shared/win32/lib* directory.

   > **Important:** Make sure the Oracle Client is working and successfully connects to the Oracle server before proceeding.

B.3.7.2 Copying the Oracle JDBC Driver

The next step is to copy the Oracle JDBC driver (class file) to the content server. You can obtain the most recent JDBC drivers for Oracle9*i* Release 2 from the Oracle Web site at `http://www.oracle.com/technology/software/tech/java/sqlj_jdbc`.

Download the file *ojdbc14.jar*, and copy this file to the directory *[CS-Install]\shared\classes*, where *[CS-Install]* is the installation directory of the Content Server instance (for example, C:*oracle\ucm\contentserver\shared\classes*).

Optionally, you can also copy the file *nls_charset12.zip* from the Oracle Web site to the Content Server location mentioned above. This file provides additional national language character set support.

   > **Important:** Make sure only one version of the Oracle JDBC driver file is in the *[Content Server_Dir]\shared\classes* directory. Remove any unnecessary driver files.

B.3.7.3 Editing the tnsnames.ora File

Tnsnames.ora is one of the network configuration files of Oracle9*i*. This file needs to be edited if you do not configure services for your database:

1. Go to the directory *[Oracle_Home]\network\admin* and open the file *tnsnames.ora* in a text editor.

2. Add the description string to this file. This could look something like:

   ```
   SERVER2.ORACLE.COM =
   ```

```
            (DESCRIPTION =
              (ADDRESS_LIST =
                (ADDRESS = (PROTOCOL = TCP)(HOST = server2.oracle.com)(PORT = 1521))
              )
              (CONNECT_DATA =
                (SERVICE_NAME = server2)
              )
          }
```

(Please note that the ADDRESS entry is on a single line.)

3. Save the modified configuration file and exit the text editor.

B.3.7.4 Editing the intradoc.cfg File

Intradoc.cfg is one of the configuration files of Content Server. This file needs to be edited to include a reference to the JDBC driver (class file) you copied earlier. To do this, complete the following steps:

1. Go to the file *[CS-Install]\bin\intradoc.cfg* (where *[CS-Install]* is the installation directory of the content server instance), and open this file in WordPad. You need to update the CLASSPATH entry (or insert it if it does not yet exist):

```
JAVA_CLASSPATH_defaultjdbc;$SharedDir/classes/ojdbc14.jar
```

where *[CS-Install]* is the installation directory of the content server instance.

> **Important:** Make sure you do not include more than one version of the Oracle classes in the class path.

2. Save the modified configuration file and exit WordPad. (If a warning is displayed about saving the file to a text-only format, click **Yes** to confirm the action.)

B.3.7.5 Copying the Oracle Shared Library File

You also need to copy the latest Oracle shared library file to the content server. To do this, complete the following steps:

1. Make a backup of the file ocijdbc9.dll, which is located in the bin subdirectory of Oracle's installation directory.

2. Go to http://www.oracle.com/technology/software/tech/java/sqlj_jdbc and download the appropriate zipped shared library/DLL file for Oracle9*i* Release 2.

3. Extract the file ocijdbc9.dll from the zip file, and copy it to the following location:

```
[Oracle_Home]\bin
```

where *[Oracle_Home]* is Oracle's installation directory.

Overwrite the existing file (you created a backup in step 1).

> **Important:** Do *not* copy this file to a location in the Content Server directory structure!

> **Note:** If you are using Oracle's Native XA (high-availability) features, you may use the file heteroxa9.dll from the downloaded zip file rather than ocijdbc9.dll. The files with '_g' in their filename are for debugging purposes only, and do not normally need to be used.

B.3.7.6 Changing the Database Settings

As the final step, you need to adjust the database settings in Content Server. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Database tab.

3. Choose the OCI driver option.

4. Specify the OCI user name and password.

5. Specify the server name, which is used by the Oracle Client to identify the Oracle server to communicate with.

6. Click **OK** to apply the setting and exit System Properties.

7. Stop and restart the Content Server (otherwise the change will not take effect).

You can now use the OCI driver to interface with the Oracle9*i* database.

B.3.8 Setting Up the Oracle OCI Driver (Oracle 10g)

Instead of the JDBC thin client for communication with Oracle 10*g*, you may also choose to use Oracle's OCI driver. If you did not select this driver during the Content Server installation, you need to set it up manually:

- Installing the Oracle Instant Client
- Copying the Oracle JDBC Driver
- Editing the intradoc.cfg File
- Changing the Database Settings

B.3.8.1 Installing the Oracle Instant Client

To install the Oracle Instant Client, complete the following steps:

1. Download the latest Instant Client software for Oracle 10*g* from http://www.oracle.com/technology/tech/oci/instantclient/ instantclient.html. The basic package will do, but you may also download any of the other packages if required (for example, the JDBC supplement because of high-availability requirements or additional language support).

2. Install the Oracle Instant Client on the computer running Content Server.

3. Configure the Oracle Instant Client so that it can successfully communicate with the Oracle server. Place the dll files into your *shared/win32/lib* directory.

> **Important:** Make sure the Oracle Instant Client is working and successfully connects to the Oracle server before proceeding.

> **Note:** It is recommended that you use Oracle's Instant Client for Oracle 10*g*. However, if you want to use OCI for other purposes than just connecting to Content Server databases, you may also use the full Oracle Client, which is included on the Oracle software distribution media.

B.3.8.2 Copying the Oracle JDBC Driver

The next step is to copy the Oracle JDBC driver (class file) to the content server. You can obtain the most recent JDBC drivers for Oracle10*g* from the Oracle Web site at http://www.oracle.com/technology/software/tech/java/sqlj_jdbc.

Download the file *ojdbc14.jar*, and copy this file to the directory *[CS-Install]\shared\classes*, where *[CS-Install]* is the installation directory of the Content Server instance (for example, C:*oracle\ucm\contentserver\shared\classes*).

Optionally, you can also copy the file *orai18n.jar* from the Oracle Web site to the Content Server location mentioned above. This file provides additional national language character set support.

> **Important:** Make sure only one version of the Oracle JDBC driver file is in the *[CS-Install]\shared\classes* directory. Remove any unnecessary driver files.

B.3.8.3 Editing the intradoc.cfg File

Intradoc.cfg is one of the configuration files of Content Server. This file needs to be edited to include a reference to the JDBC driver (class file) you copied earlier. To do this, complete the following steps:

1. Go to the file *[CS-Install]\bin\intradoc.cfg* (where *[CS-Install]* is the installation directory of the content server instance), and open this file in WordPad. You need to update the CLASSPATH entry (or insert it if it does not yet exist):

   ```
   JAVA_CLASSPATH_defaultjdbc;$SharedDir/classes/ojdbc14.jar
   ```

   where *[CS-Install]* is the installation directory of the content server instance.

   > **Important:** Make sure you do not include more than one version of the Oracle classes in the class path.

2. Save the modified configuration file and exit WordPad. (If a warning is displayed about saving the file to a text-only format, click **Yes** to confirm the action.)

B.3.8.4 Changing the Database Settings

As the final step, you need to adjust the database settings in Content Server. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Database tab.

3. Choose the OCI driver option.

4. Modify the JDBC connection string to suit your specific application. Use the following string format:

```
jdbc:oracle:oci:@[host]:[port]:[Oracle_instance]
```

For example:

```
jdbc:oracle:oci:@csdb4:1521:ucm1
```

5. Specify the OCI user name and password.

6. Specify the server name, which is used by the Oracle Instant Client to identify the Oracle server to communicate with.

7. Click **OK** to apply the setting and exit System Properties.

8. Stop and restart the Content Server (otherwise the change will not take effect).

You can now use the OCI driver to interface with the Oracle 10*g* database.

B.4 Setting Up Sybase

If you chose to set up Sybase manually during the installation of the Content Server software, you need to complete the following :

- Creating the Content Server Database
- Creating the Database Tables
- Configuring the JDBC Settings
- Specifying the Classpath
- Rebuilding the Content Server Portal Page
- Restarting the Server(s)

B.4.1 Creating the Content Server Database

If you did not already create the Content Server database in Sybase, you need to do so. Refer to Chapter 3, "Pre-Installation Tasks and Considerations" for further guidelines and considerations.

B.4.2 Creating the Database Tables

You need to create the database tables in the Content Server database. This is accomplished by running a series of SQL scripts that are shipped with the Content Server software. If the content server tables already exist, they will be dropped and re-created.

> **Important:** Make sure the default database is the content server database. If it is not, the script operations below will be performed on the incorrect database.

To create the Sybase database tables, complete the following steps:

1. Change your working directory to either of the following:

   - For **non-Unicode text fields** (varchar) in the database tables:
     [CS-Install]\database\sybase

- For **Unicode text fields** (nvarchar) in the database tables:
  [CS-Install]\database\sybase\unicode

(where *[CS-Install]* is the installation directory of the content server instance).

2. Start *isql.exe* and log in to the database using the Sybase user name and password for the content server.

3. Run the scripts in the appropriate directory (Unicode or non-Unicode) by entering the following commands on the command line (in the order shown):

```
isql -i intradoc.sql
isql -i default.sql
isql -i formats.sql
isql -i format_defaults.sql
isql -i users.sql
isql -i workflow.sql
```

where *[CS-Install]* is the installation directory of the content server instance.

> **Note:**   If you are setting up Sybase *before* installing the Content Server software, then the SQL scripts are available on the software distribution media, in the *UCM**ContentServer**database**sybase* directory (and its *unicode* subdirectory).

> **Note:**   You may get error messages because these procedures try to delete tables that do not yet exist in an initial installation. You may safely ignore these error messages.

4. While still in isql, also run the following script:

```
[CS-Install]\database\sybase\admin\rowlocking.sql
```

(where *[CS-Install]* is the installation directory of the content server instance). This script converts the database from table locking to row locking, which reduces potential deadlocks of the Sybase database.

5. When all scripts have been completed, exit isql.

B.4.3 Configuring the JDBC Settings

For the content server to communicate with Sybase successfully, you need to configure the JDBC settings in Content Server. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Database tab.

3. Select the following options:

   - Use Java Database Connectivity

   - Sybase JDBC Driver

4. Modify the JDBC connection string to suit your specific application. Use the following string format:

```
jdbc:sybase:Tds:[DB_Host_Name]:[DB_Server_Port]/[DB_Name]
```

where *[DB_Host_Name]* is the host name of the Sybase server, *[DB_Server_Port]* is the port number (usually 5000), and *[DB_Name]* is the Content Server database name, for example:

```
jdbc:sybase:Tds:cssybase:5000/oracle
```

5. Also provide the JDBC user name and password as required. These are the user name and password used to connect to the Sybase database.

> **Note:** The JDBC user name and password should be same as the one used to create the Sybase tables. If the JDBC user does not have access privileges to the tables, the content server will fail to start.

6. Click **OK** to save the changes and exit the System Properties utility.

B.4.4 Specifying the Classpath

For the content server to communicate with Sybase successfully, you need to provide a reference to the JDBC driver file that is used with the database. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

The System Properties applet is started.

2. Open the Paths tab.

3. Specify the following as the classpath:

```
JAVA_CLASSPATH_defaultjdbc;$SharedDir/classes/jconn3.jar
```

4. Click **OK** to save the changes and exit the System Properties utility.

B.4.5 Rebuilding the Content Server Portal Page

You need to rebuild the content server portal page. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **Weblayout Editor**.

The System Properties applet is started.

2. Choose Update Portal from the Options menu.

3. Click **OK**.

B.4.6 Restarting the Server(s)

As the final step, you need to (re)start the content server. If the database is installed on a proxied server, make sure that you restart the content servers in the following order:

1. Restart the proxied server that the Sybase database was installed on.

2. Restart the master server.

3. Restart the proxied server again.

Sybase is now ready for use with Content Server.

B.5 Setting Up DB2

If you chose to set up DB2 manually during the installation of the Content Server software, you need to complete the following:

- Copying the DB2 JDBC Driver Files
- Creating the Content Server Database
- Creating the Database Tables
- Configuring the JDBC Settings
- Specifying the Classpath
- Turning Off Next Key Locking
- Preserving Database Case
- Rebuilding the Content Server Portal Page
- Restarting Servers

> **Note:** Full-text search and indexing for DB2 are not supported in this Content Server version.

B.5.1 Copying the DB2 JDBC Driver Files

The first step in setting up IBM DB2 for use with Content Server is to copy the DB2 JDBC driver. Copy the files

```
[DB2_Dir]\sqllib\java\db2jcc_license_XX.jar
[DB2_Dir]\sqllib\java\db2jcc.jar
```

(where *[DB2_Dir]* is DB2's program root directory, and 'XX' a two-letter platform code, which is typically 'CU')

to the following directory:

```
[CS-Install]\shared\classes
```

(where *[CS-Install]* is the installation directory of Content Server).

> **Important:** If you update DB2 and this process updates the DB2 JDBC driver files, make sure that you copy the new files to the Content Server shared classes directory so the driver version exactly matches the database version.

> **Note:** The above step works if DB2's default JVM and Java-related classes are used on the DB2 server (this will be true in the majority of cases). If the DB2 administrator chose to use a non-default JVM and Java-related classes for DB2, you need to make sure that the JDBC driver version on the clients *exactly* matches that of the DB2 applet server.

B.5.2 Creating the Content Server Database

If you did not already create the Content Server database in DB2, you need to do so. To create the database and connect to it, run the following commands in the DB2 Command Window:

```
db2 CREATE DB [DB-Name] ALIAS [DB-Alias]
db2 CONNECT TO [DB-Alias] USER [User] USING [Password]
```

> **Important:**   Do not use the Command Line Processor or the Control Center.

> **Note:**   In the lines above, *[DB-Name]* is the database name and *[DB-Alias]* the database alias.
>
> Both the database name (*DB-Name*) and database alias (*DB-Alias*) may not be longer than 8 characters.

B.5.3 Creating the Database Tables

You need to create the database tables in the Content Server database. This is accomplished by running a series of SQL scripts that are shipped with the Content Server software. If the content server tables already exist, they will be dropped and re-created.

The script files are located in the following two locations:

- To create **non-Unicode text fields** (varchar) in the database tables:

  `[CS-Install]\database\db2`

- To create **Unicode text fields** (nvarchar) in the database tables:

  `[CS-Install]\database\db2\unicode`

To create the DB2 database tables, run the following scripts in the DB2 Command Window (in the order provided), using the `-tvf` parameter:

- intradoc.sql
- default.sql
- formats.sql
- format_defaults.sql
- users.sql
- workflow.sql

> **Important:**   Both of the above script directories also contain an SQL script called *dropall.sql*. Do not run this script as it drops all database tables!

> **Note:** If you are setting up DB2 *before* installing the Content Server software, then the SQL scripts are available on the software distribution media, in the *\UCM\ContentServer\database\db2* directory (and its *unicode* subdirectory).

B.5.4 Configuring the JDBC Settings

For the content server to communicate with DB2 successfully, you need to configure the JDBC settings in Content Server. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Database tab.

3. Select the following options:

   - Use Java Database Connectivity

   - Other JDBC Driver

4. Specify the following as the JDBC driver name:

   ```
   COM.ibm.db2.jcc.DB2Driver
   ```

5. Specify the following as the JDBC connection string:

   ```
   jdbc:db2://[DB2_Host_Name]:[DB_Server_Port]/[DB_Alias]
   ```

   where *[DB2_Host_Name]* is the host name of the DB2 server, *[DB_Server_Port]* is the port number (50000 by default), and *[DB_Alias]* is the Content Server database alias, for example:

   ```
   jdbc:db2://csdb2:50000/oracle
   ```

6. Also provide the JDBC user name and password as required. These are the user name and password used to connect to the DB2 database.

   > **Note:** The JDBC user name and password should be same as the one used to create the DB2 tables. If the JDBC user does not have access privileges to the tables, the content server will fail to start.

7. Click **OK** to save the changes and exit the System Properties utility.

B.5.5 Specifying the Classpath

For the content server to communicate with DB2 successfully, you need to provide a reference to the JDBC driver files that are used with the database. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then **Content Server-[Instance-Name]**, then **Utilities**, and then **System Properties**.

   The System Properties applet is started.

2. Open the Paths tab.

3. Specify the following as the classpath:

```
JAVA_CLASSPATH_defaultjdbc;$SharedDir/classes/db2jcc.jar;
$SharedDir/classes/db2jcc_license_cu.jar
```

(Please note that this is all on a single line.)

4. Click **OK** to save the changes and exit the System Properties utility.

B.5.6 Turning Off Next Key Locking

Make sure that you set the following DB2 environment variable:

```
db2set DB2_RR_TO_RS=on
```

> **Important:**   Make sure that you use 'on' as the value, not 'YES' (as reported incorrectly by some IBM administration guides).

If you do not set the above environment variable, transaction deadlocks and timeouts may be reported. The above environment variable turns off Next Key Locking, which is known to cause concurrency issues. Next Key Locking is used in DB2's transaction isolation mechanism, Repeatable Read (RR). It basically places locks not only on the current row, but also the row containing the next key in an index, in order to prevent phantom reads (which means the result set could grow in two consecutive reads because a second thread has changed a different row to match the query criteria). This implicit locking could cause two seemingly unrelated transactions to clash and form a deadlock. This potential deadlock problem can be resolved by turning the above DB2 environment variable on.

B.5.7 Preserving Database Case

Make sure that you preserve the database case for DB2. This is done by turning on a setting in Content Server. If you do not do this, you will not be able to start the content server. To turn on the required setting in Content Server, do the following:

1. From the Windows **Start** menu, select **Programs**, then
Content Server-[Instance-Name], then **Utilities**, and then **System Properties**.

The System Properties applet is started.

2. Open the Database tab.

3. Make sure the Enable database preserve case check box is selected.

4. Click **OK** to apply the change and exit the System Properties utility.

B.5.8 Rebuilding the Content Server Portal Page

You need to rebuild the content server portal page. To do this, complete the following steps:

1. From the Windows **Start** menu, select **Programs**, then
Content Server-[Instance-Name], then **Utilities**, and then **Weblayout Editor**.

The Weblayout Editor applet is started.

2. Choose **Update Portal** from the Options menu.

3. Click **OK**.

B.5.9 Restarting Servers

As the final step, you need to (re)start the content server. If the database is installed on a proxied server, make sure that you restart the content servers in the following order:

1. Restart the proxied server that the DB2 database was installed on.

2. Restart the master server.

3. Restart the proxied server again.

DB2 is now ready for use with Content Server.

C

Content Server Components

This appendix covers the components that are shipped with the Content Server 10*g*R3 software:

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

C.1 About Content Server Components

The Content Server software is shipped with a number of components, which are modules of program code, resources, and templates that are designed to interact with the content server at runtime. They add or modify functionality to the content server without affecting the core.

This appendix addresses components that are installed or offered as an option during the time of Content Server installation. It does not address components distributed as extras or used in product distributions other than Content Server. See the release notes for more information about component updates.

> **Note:** See the Content Server developer documentation for more information on components.

C.2 Component Installation Status

Some components are always installed with the Content Server 10gR3 software, while others are optional and need to be specifically selected for installation. Also, some components are considered system components, and should never be disabled or uninstalled.

Some components are installed and enabled by default, but do not function until configured. These components can be disabled or uninstalled prior to configuration, but once they are configured, they should not be installed—for example, FileStoreProvider.

Other components can be disabled provided they are not needed to support other installed components—for example, InboundRefinerySupport. See the table below for details.

Component Name	Installed?	Enabled (default)	Standard / System Component	May Be Disabled or Uninstalled
ActiveDirectoryLdapComponent	Always	Yes	No	Yes, unless Content Server using LDAP
AddCCToArchiveCheckin	Optional	No	No	Yes unless Content Categorizer is installed and enabled
AddCCToNewCheckin	Optional	No	No	Yes unless Content Categorizer is installed and enabled
ArchiverReplicationExceptions	Always	Yes	Yes	Yes
CheckOutAndOpenInNative	Always	Yes	No	Yes, until configured for use
CheckSCSHealth	Always	Yes	Yes	Yes
CIS_Helper	Always	Yes	Yes	Yes, unless Content Integration Suite is used
ComponentTool	Always	Yes	Yes	Yes
ConfigMigrationUtility	Always	Yes	Yes	Yes
ContentAccess	Always	Yes	No	Yes, unless Dynamic Converter is used
ContentCategorizer	Optional	No	No	Yes
ContentFolios	Optional	Yes	No	Yes, until configured for use
ContentTracker	Optional	No	No	Yes
ContentTrackerReports	Optional	No	No	Yes
CoreUserInterfaceLibrary	Always	Yes	Yes	No
CoreWebDav	Always	Yes	Yes	Yes, until configured for use
DBSearchContainsOpSupport	Always	Yes	Yes	Only if not using Oracle database
ExtendedUserAttributes	Optional	Yes	Yes	Yes
FCKEditor	Always	Yes	Yes	Yes, unless FormEditor is used
FileStoreProvider	Always	Yes	No	Yes, until configured for use

Component Name	Installed?	Enabled (default)	Standard / System Component	May Be Disabled or Uninstalled
Folders_g	Optional	Yes	No	Yes
FormEditor	Always	Yes	No	Yes, until configured for use
InboundRefinerySupport	Always	Yes	No	Yes if Content Server not using Inbound Refinery
iTextComponent	Always	Yes	Yes	No
LinkManager8	Optional	Yes	No	Yes
Localization	Always	Yes	Yes	Yes if Content Server instance is English Only
NativeOsUtils	Always	Yes	Yes	No
OracleQueryOptimizer	Oracle DB only	Yes	No	Yes if not using Oracle database
OracleTextSearch	Optional	Yes	No	Yes if Content Server not configured for full-text search
PopUpCalendar	Always	Yes	Yes	No
PDFWatermark	Optional	No	No	Yes
ProxyConnections8	Always	Yes	Yes	Yes, until configured for use
SecurityProviders	Always	Yes	No	No
ThreadedDiscussions	Optional	Yes	No	Yes
UserProfileSchemaLoader	Always	Yes	Yes	No
WebUrlMapPlugin	Always	Yes	Yes	No
WsdlGenerator	Always	Yes	Yes	Yes
YahooUserInterfaceLibrary	Always	Yes	Yes	No

Standard and system components are not shown in the list of installed components if the "Hide Standard and System Components" check box is selected on the Component Manager page in Content Server.

All components, except ContentAccess and NativeOsUtils, are included in the *\packages\allplatform* directory of the Content Server 10*g*R3 distribution package. The ContentAccess and NativeOsUtils components are platform-specific; they are located in the *\packages\win32* directory (for example,).

C.3 ActiveDirectoryLdapComponent

The ActiveDirectoryLdapComponent component is an extension to the basic Content Server LDAP (Lightweight Directory Access Protocol) provider. It enables the content

server to use an LDAP provider to authenticate users against information stored in a Microsoft Active Directory server. The provider pulls in group membership and specified user metadata from Active Directory.

Using Active Directory with LDAP may be the preferred approach if your network includes the following:

- Content Server access is through non-Internet Explorer client browsers.

- Content Server is installed on a UNIX operating system.

- Content Server is installed on a Windows operating system that is using a web server other than IIS.

- A firewall is used between the content server and user base computers.

> **Note:** You can find more information about LDAP authentication in the following document: *[CS-Install]\weblayout\help\ documentation\admin\managing_security_10en.pdf*.

C.4 AddCCToArchiveCheckin

When AddCCToArchiveCheckin component is installed and enabled, the ARCHIVE_ CHECKIN_NEW service is modified to call Content Categorizer when a batch file is run to load content. This means files loaded into Content Server using Batchloader are categorized automatically.

C.5 AddCCToNewCheckin

When AddCCToNewCheckin component is installed and enabled, the CHECKIN_ NEW and CHECKIN_UNIVERSAL services are modified to call Content Categorizer at time of content check in. This means a file copied to a WebDAV folder using Windows Explorer is categorized automatically when checked in. Similarly, a user can save a step by clicking Check In on a Check In page in Content Server instead of Categorize, and the content is categorized automatically.

C.6 ArchiverReplicationExceptions

The ArchiverReplicationExceptions component enables administrators to prevent failed imports from stopping replication. It does this by capturing such failed imports, putting them into an "exceptions" archive, and sending out e-mail to the administrator that such a failed import has occurred.

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\ArchiverReplicationExceptions\ install_admin_ARE_10.pdf*.

C.7 CheckOutAndOpenInNative

The CheckOutAndOpenInNative component enables users to check out and open content items in WebDAV-compliant applications directly from the content server.

End-users can directly check out and open content items from the content server using the Check Out and Open options on search results pages and content information pages. Content items open in their native application if the application is

WebDAV-compliant (for example, Microsoft Word). Users can edit a content item and check it back into the content server using that application. Each time they save the content item in the native application, a new revision of the item is checked into the content server.

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\CheckoutAndOpenInNative\check_out_and_open.pdf*.

C.8 CheckSCSHealth

The CheckSCSHealth component adds the following services for use with the content server:

- **CHECK_SEARCH_HEALTH:** This service runs a search to ensure that the search engine is functioning. If 'QueryText' is not passed in the request, a blank search is run.

- **CHECK_FS_HEALTH:** This service creates a file on all known file systems, including the *vault*, *weblayout*, *data*, and *shared* directories of the content server instance.

- **CHECK_PROVIDER_HEALTH:** This service tests the health of all known providers. 'pName' must be passed in the request ('SystemDatabase', 'SystemServerSocket', etc.).

- **CHECK_ALL_HEALTH:** This service checks the health of all providers, the file system, and the search engine.

If the status code returned is less than 0 (zero), an error occurred.

These services are mainly useful when integrating the content server with a third-party monitoring utility, such as Nagios (*http://www.nagios.org*). The component includes a Perl script that can be used as a Nagios plugin (in the component's 'perl' subdirectory). It can also be modified to run with a different third-party monitoring tool.

> **Note:** You can find more information about this component (including instructions on integrating the new services with the Nagios monitoring utility) in the following file: *[CS-Install]\custom\CheckSCSHealth\readme.txt*.

C.9 CIS_Helper

The CIS_Helper component is used by Content Integration Suite (CIS). It helps parse method calls between the content server and the CIS layer. It contains a few services that are used when calling Content Server via the CIS APIs. Specifically, the component has services to allow for streaming of Dynamic Converter responses into application server environments and to support additional configuration options for file transfers in certain CIS configurations.

C.10 ComponentTool

The ComponentTool component provides a command-line tool for installing, enabling, and disabling Content Server components.

After installing this component, create a symlink or copy of the launcher:

```
cd bin && copy IdcServer.exe ComponentTool.exe
```

Usage of the component is as follows:

```
ComponentTool --install|--enable|--disable path|name
ComponentTool --list-enabled|--list-disabled|--list|--help
```

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\ComponentTool\readme.txt*.

C.11 ConfigMigrationUtility

The ConfigurationMigrationUtility component can be used to select elements of a content server instance for migration to another instance. It enables system administrators to export and import bundles of Content Server specific configurations.

You can select individual elements (such as workflow tokens or content types) or entire sections (such as all user-related metadata or all metadata related to workflows). In addition, you can export and import an entire content server in order to create a snapshot of the content server at a certain point in time. It can be used to migrate a system from testing to production, or to provide an upgrade path from versions of the content server. By using the migration tool, you can keep an older version of the content server in production while testing new functionality on a newer version.

Each export configuration is packaged as a bundle which contains the information needed to re-create the configuration on another system. A bundle is a zip file that can be easily shared with other systems.

> **Note:** Documentation for the Configuration Migration Utility is included in the content server's online help for system administrators, and is also available as a PDF file in *[CS-Install]\weblayout\help\documentation\admin\sysmigration_cserver_10en.pdf*.

C.12 ContentAccess

The ContentAccess component provides the Outside In filters that are used to convert native content items (for example, Microsoft Word documents) to web-viewable formats (for example, HTML or PDF files). In addition, it provides full-text extraction capability. It is a system component, and should never be disabled or uninstalled.

> **Note:** The ContentAccess component is different for each supported platform. Its zip file is located in the *\packages\[os_name]* directory of the Content Server distribution package.

C.13 ContentCategorizer

Suggests metadata values for documents being checked into the Content Server instance, and it can be used to recategorize the metadata of documents that are already in. Metadata values are determined according to search rules provided by the administrator.

C.14 ContentFolios

The Content Folios component provides a quick and effective way to assemble, track, and access logical groupings of multiple content items from within the secure environment of Content Server. For example, all items relevant to an upcoming brochure, such as images, logos, legal disclosures, and ad copy, can be assembled and sent through a workflow process. Once approved, all associated content can be downloaded and sent for print. Or perhaps a new project requires a virtual place to assemble all relevant content items in a particular hierarchy, whenever they are checked in, with restricted access to particular areas of the hierarchy. Or a video may need to be associated and tracked with release waivers and narration text. All this can be done with Content Folios.

Technically, a content folio is an XML file checked into the content server that uses elements to define a hierarchical structure of nodes, slots, and specified content items in the content server. In practice, a content folio is a logical grouping, or a framework in which content stored in Content Server can be structured. Simple folios are a flat container, while advanced folios can nest content in a hierarchy within folders. In an advanced folio, the hierarchy may be established prior to assembling content items, or it may be created during or subsequent to assembling the items. Existing folios can have content added to them, or can be locked so that no changes can be made. Content items can be added to a simple folio by searching Content Server, and to an advanced folio by checking new items into the content server repository or by searching for content that has previously been checked in, all through the folio interface. An advanced folio can even contain hyperlinks to outside resources such as web sites or shared network drives.

> **Note:** You can find more information about this component in the following file: *[CS-Install]\weblayout\help\documentation\ admin\ admin_guide_folios_10en.pdf*.

C.15 ContentTracker

Monitors activity on the Content Server instance and records selected details of those activities. It then generates reports that can help administrators understand the ways in which the system is being used.

C.16 ContentTrackerReports

Reports on the data generated by the Content Tracker component.

C.17 CoreUserInterfaceLibrary

The CoreUserInterfaceLibrary component includes shared JavaScript and dynamic HTML pages for use by a number of other components. It is a system component, and should never be disabled or uninstalled.

C.18 CoreWebDav

The CoreWebDav component enhances the content server to allow it to respond to DAV (Distributed Authoring and Versioning) requests, which provides a way to remotely author and manage your content using clients that support the WebDAV protocol. For example, contributors can use Windows Explorer or Microsoft Office

products to check in, check out, and modify content in the repository rather than using Content Server's own web browser interface.

In a typical Content Server 10*g*R3 installation, the WebDav component causes the server to respond to `http://[Server-Host]/[Instance-Name]/idcplg/webdav` requests.

> **Note:** You can find more information about this component, including some installation considerations, in the following file: *[CS-Install]\custom\CoreWebdav\readme.html*.

> **Important:** There is also a WebDav component, which is specifically intended for pre-10*g*R3 Content Server releases. If this component is enabled on your content server (for example, after a system upgrade), then make sure that you disable it. Otherwise, the WebDAV functionality will not work on your content server.

C.19 DBSearchContainsOpSupport

The DBSearchContainsOpSupport component adds support of the hasAsWord (Contains) operator to database searching and indexing, both metadata-only and full text (if supported by the database):

For SQL Server and Oracle, follow the "Zone Fields Configuration" link on Administration page to define indexes that would be full-text indexed. Zone fields are searchable with the hasAsWord operator.

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\DBSearchContainsOpSupport\readme.txt*.

> **Important:** Changing a text field to a zone text field can be a very time-consuming operation. The amount of time it takes to parse the text and create the full-text index depends on the number of content items in the content server and the amount of text stored in the text field. However, once the text field has been indexed, you should not experience significant performance issues when updating and adding content items.

C.20 ExtendedUserAttributes

The ExtendedUserAttributes component enables administrators to add extended attributes to a user. These attributes are merged into pre-existing attributes, but allow additional flexibility in management.

When this component is installed, the following new services are available:

- **ADD_EXTENDED_USER_ATTRIBUTES**: This service adds extended user attributes to a user. The user does not have to exist before using the service. If this service is asked to add extended attributes which already exist for the user, the service modifies the previous entries.

- **EDIT_EXTENDED_USER_ATTRIBUTES**: This service edits extended user attributes for a user. The user does not have to exist before using the service. All previously extended attributes are replaced by the new extended attributes provided.

- **DELETE_EXTENDED_USER_ATTRIBUTES**: This service deletes specific extended user attributes for a user.

- **DELETE_EXTENDED_ATTRIBUTES_BY_APPLICATION**: This service deletes all extended attributes for a particular role/account for a specified application.

- **DELETE_ALL_EXTENDED_ATTRIBUTES_FOR_USER**: This service deletes all extended attributes for a user.

- **DELETE_EXTENDED_ATTRIBUTES_FOR_APPLICATION**: This service deletes all extended users attributes for an application.

- **QUERY_EXTENDED_USER_ATTRIBUTES**: This service places all of a user's extended attributes into a result set in the binder. All of the data is put into the ExtUserAttribInfo result set.

- **EC_SET_PROPERTY**: This service sets an extended configuration property. It can be used to either add a new property or modify an existing property.

- **EC_DELETE_PROPERTY**: This service deletes an extended configuration property. It is important that the exact key be specified for deletion. This service does not automatically delete all subkeys under a key.

- **EC_GET_PROPERTY**: This service returns a specified extended configuration property in the result set PROPERTY_LIST. It is important that the exact key be specified; if you want to search based on just the key (not subkey) use EC_GET_ PROPERTY_BY_KEY.

- **EC_GET_PROPERTY_BY_KEY**: This service returns a specified extended configuration property in the result set PROPERTY_LIST.

- **SET_DEFAULT_ATTRIBUTES**: This service sets some default attributes that will always be applied to a user. The type is "defaults" and the key is "userattributes", so these do not need to be provided.

- **DELETE_DEFAULT_ATTRIBUTES**: This service deletes some default attributes that will always be applied to a user.

- **GET_DEFAULT_ATTRIBUTES**: This service returns the default attributes that are applied to all users in the DEFAULT_ATTRIBUTES result set.

In addition, the following existing services are modified:

- **ADD_USER**: This service has been altered to add extended user attributes at the same time the user is added.

- **EDIT_USER**: This service has been altered to allow editing of extended user attributes at the same time. The old values are completely replaced by the new ones.

- **DELETE_USER**: This service has been altered to delete a user's extended attributes if they exist.

- **QUERY_USER_ATTRIBUTES**: This service acts as usual however the attributes it returns are a merger of both regular and extended user attributes.

C.21 FCKEditor

The FCKEditor component provides the JavaScript libraries needed to run FCKeditor, which is a light-weight JavaScript-based HTML text editor that does not require any kind of installation on the client computer. This component is required for the Web Form Editor (FormEditor component), and can also be used to implement lightweight HTML text editors in content server customizations.

> **Note:** You can find more information about FCKeditor on the following web site: www.fckeditor.net.

C.22 FileStoreProvider

The FileStoreProvider component extends the standard file storage and organization mechanism that ships with the Content Server core to include a number of enhancements that are particularly useful for very large systems. It exposes the file store functionality in the Content Server interface, and allows additional configuration options. For example, you can configure Content Server to use large object (LOB) datatypes to store content in a database, instead of using a file system. This offers several advantages: it integrates repository management with database management for consistent backup processes; can help overcome limitations associated with directory structure and number of files per directory in a file system approach; and aids in distributing content more easily across systems, for better scaling of Content Server. Additionally, the FileStoreProvider component allows the use of different types of storage devices not commonly associated with a file system (for example, content addressed storage systems and write-only devices necessary in some business uses).

> **Caution:** FileStoreProvider should not be uninstalled or disabled once it is installed and the default file store is upgraded. If you install FileStoreProvider during the standard Content Server installation and do not upgrade the default file store, you can uninstall the component following the procedures contained in the *File Store Provider Installation and Administration Guide*.

> **Note:** Documentation for File Store Provider is included in the content server's online help for system administrators, and is also available as a PDF file in *[CS-Install]\weblayout\help\documentation\admin\admin_FS_provider_10en.pdf*.

C.23 Folders_g

The Folders_g component provides a hierarchical folder interface to content in Content Server in the form of "virtual folders" (also called "hierarchical folders"), similar to the folders tree in Windows Explorer. Virtual folders enable you to create multi-level folder structures.

Virtual folders provide a number of benefits:

- Users can find content by drilling down through a familiar folder-type interface.

- Users can apply default metadata to content items by checking them in through a particular folder.

■ The system administrator can control the default metadata applied to content items by appropriately setting up folders. In turn, the preset default metadata is applied to content items when users check them in through a particular folder (set up by the system administrator).

> **Note:** Documentation for Folders_g is included in the content server's online help for system administrators, and is also available as a PDF file in *[CS-Install]\weblayout\help\documentation\admin\admin_folders_webdav_10en.pdf*.

C.24 FormEditor

The FormEditor component provides a cross-platform, browser-based visual design environment to create Hypertext Web Form Editor Files (HCSFs) and associated Idoc resources.

HCSFs can be used to create HTML forms with XML-formatted Idoc Script and/or other script code that can be checked into the content server and completed by content consumers. The XML data set of each completed form is checked into the content server as a separate content item (HCSP file with the submitted data embedded in XML).

These HCSP files are full-text indexed and can be processed further (for example, using workflows or subscriptions).

IDOC files contain HTML and Idoc Script resources that can be loaded and displayed on HCSF files.

The Web Form Editor is tightly integrated into Content Server, which enables you to select metadata fields for presentation on the form and save the form definition into the content server from the editor interface. In addition, Content Server includes can be used to display both XML data island fields and Content Server metadata fields. The Web Form Editor uses the includes normally used on check-in, update, info, and search pages. This means that if a Content Server field is used on a form, it will be displayed according to Content Server rules. For example, if a field is associated with a view, it will be displayed with its view.

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\FormEditor\web_form_editor_10en.pdf*.

C.25 InboundRefinerySupport

The InboundRefinerySupport component adds functionality and some configuration options to Content Servers that connect to one or more Inbound Refinery or refineries.

C.26 iTextComponent

The iTextComponent component provides a PDF distribution library to allow components to share PDF documents.

C.27 LinkManager8

The LinkManager8 component extracts URL links of indexed documents, and evaluates, filters, and parses the URLs according to a pattern engine. The results are subsequently stored in a database table. Currently, the component uses HtmlExport to convert the file, if necessary, to a parsable (i.e., text) format. Since the link extraction happens during the indexing cycle, only the links of released documents are managed. This means that for multiple revisions only the most recent revision can have entries in the table.

The component enhances the browser user interface to allow searching and management of the links table.

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\LinkManager8\readme.txt*.

C.28 Localization

The Localization component contains the localization resources for Content Server, Refinery, Records Manager, and a number of other components. The available languages are:

- Arabic (ar)
- German (de)
- English (en)
- Spanish (es)
- French (fr)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Dutch (nl)
- Portuguese (Brazil) (pt.br)
- Thai (th)
- Chinese (Simplified) (zh.cn)
- Chinese (Traditional) (zh.tw)

C.29 NativeOsUtils

The NativeOsUtils component provides the Java wrapper for native calls to various native OS methods that are not provided by the Java VM. This includes Windows registry manipulation, toggling execution state on UNIX files, doing soft/hard file links, Windows inter-process communication, and various other small little OS APIs.

> **Note:** The NativeOsUtils component is different for each supported platform. Its zip file is located in the *\packages\[os_name]* directory of the Content Server distribution package.

C.30 OracleQueryOptimizer

The OracleQueryOptimizer component helps large content server installations that use an Oracle database. It analyzes static queries (defined as resources) and data sources, and optimizes problematic queries and data sources with Oracle-specific hints. It also includes changes for ExpiredContent and Indexer to remove inefficient queries.

In addition, the component provides a dynamic query optimizer to examine the queries to be executed with a data source and through the JDBC workspace. This optimizer parses out queries and *where* clauses for data sources, and picks out the best hint according to a rule table. The selected hints are then added to the query before it is executed.

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\OracleQueryOptimizer\readme.html*.

C.31 OracleTextSearch

The OracleTextSearch component enables the user of Oracle Text as the primary full-text search engine for Universal Content Management (UCM), matching or exceeding the search capabilities offered by UCM with Autonomy VDK. The component enables administrators to specify certain metadata fields to be optimized for the search index and to customize additional fields. The component also enables a fast index rebuild and index optimization.

OracleTextSearch component is installed and enabled by default, but must be configured after installing in order to function properly. For more information about post-installation procedures, see the *Oracle Text Search Administration* guide.

C.32 PDFWatermark

Enables watermarks to be applied to PDF files generated by the Inbound Refinery PDFConverter component and returned to the Content Server system. PDF files already residing on the Content Server system also can be watermarked. Dynamic watermarks are generated on-the-fly and can contain variable information.

C.33 PopUpCalendar

The PopUpCalendar component causes a calendar icon to be displayed to the right of all date fields on the content server's check-in and update pages. If a user clicks the icon, a calendar dialog pops up and the user can click a date to select it. The dialog loads the selected date into the associated input field on the parent page. This component enables users to quickly select dates and easily move between previous and future months and years. It also eliminates date formatting and typographical errors because the component automatically populates date fields with the user-selected dates.

The component may also be configured to display the dialog via JavaScript without popping open a window.

The date format displayed by the component is controlled by the date format property of the user locale. Any date strings are also localized, when a corresponding translation string exists in the *wwstrings.htm* file.

> **Note:** You can find more information about this component in the following files: *[CS-Install]\custom\PopUpCalendar\readme.txt* and *admin_guide_popupcal_752en.pdf* (in that same directory).

C.34 ProxyConnections8

The ProxyConnections8 component provides a user interface for creating password-protected connections to a content server or for creating credential maps. The credential maps can also be used to map credentials from an external source (specifically NT integration solutions including the ADSI integration).

In addition, the ProxyConnections8 component adds the ability to proxy a content server using the HTTP protocol. The component adds an httpoutgoing provider, which allows communication from one content server (the master) to the other (the proxy). In particular, all static URL requests to *weblayout/groups/* are forwarded to another web server, thus creating a proxy at the web server level (as well as the usual one at the content server level).

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\ProxyConnections8\readme.txt*.

C.35 SecurityProviders

The SecurityProviders component provides SSL encryption and authentication on the standard Content Server incoming and outgoing socket providers. The component extends the basic socket providers in two ways. First, it adds SSL security and authentication to the socket layer. In addition, since the creation and teardown of SSL sockets can be expensive, the SSL incoming and outgoing provider are designed to use keepalive and connection pooling logic. This helps to avoid SSL overhead.

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\SecurityProviders\readme.txt*.

C.36 ThreadedDiscussions

The ThreadedDiscussions component enables creating discussion documents about another document. It takes any regular document and adds '_d' to the content ID to create a new HCSP-style document that is focused on a discussion about the originating document.

> **Note:** You can find more information about this component in the following file: *[CS-Install]\custom\ThreadedDiscussions\readme.html*.

C.37 UserProfileSchemaLoader

The UserProfileSchemaLoader component enables administrators to create views of user profile data. This component is used by the ContentFolios component. It is a system component that should never be disabled or uninstalled.

C.38 WebUrlMapPlugin

The WebURLMapPlugin component allows URLs to be mapped to other URLs in the content server using a simple substitution script for the mapping.

You can edit the Web URL map by clicking the associated link at the bottom of the Filter Administration page.

> **Note:**   You can find more information about this component in the following files: *[CS-Install]\custom\WebUrlMapPlugin\readme.txt* and *[CS-Install]\weblayout\help\documentation\admin\managing_system_10en.pdf*.

C.39 WsdlGenerator

The WsdlGenerator component enables users to request SOAP-based messages and receive SOAP-based responses. The component supports two formats: a generic format that closely resembles the Content Server DataBinder object, and a custom format that can be encapsulated in WSDLs to be used as web services in other applications. In addition, the component also supports two multi-part formats: SOAP with Attachments, and SOAP with DIME. These formats allow file content to be uploaded to, and downloaded from, the content server in message attachments separate from the actual SOAP messages.

> **Note:**   You can find more information about this component in the following files: *[CS-Install]\custom\WsdlGenerator\soap.txt* and *[CS-Install]\weblayout\help\ documentation\addons\soap_wsdl_10en.pdf*.

C.40 YahooUserInterfaceLibrary

The YahooUserInterfaceLibrary component provides a set of utilities and controls, in JavaScript, for building richly interactive web applications using techniques such as DOM scripting, DHTML and Ajax. It also includes several core CSS resources. This component is a system component, and should never be disabled or uninstalled.

D

Setting Up Database Search and Indexing

By default, Content Server 10*g*R3 is set up to use the database to provide searching and indexing capabilities. The out-of-the-box database configuration provides metadata-only searching and indexing. However, you can modify the default configuration of Oracle and SQL Server to enable full-text searching and indexing (see "Setting Up the Database for Full-Text Searching/Indexing" on page D-3). Sybase and DB2 only support metadata searching and indexing.

Add-ons are available which allow different search solutions to be integrated with Content Server (for example, Verity or FAST). Separate integration documentation is available for each supported search solution.

D.1 Database Search and Indexing Considerations

Please note the following important considerations with regard to database search and indexing:

- All Databases

- Oracle

- SQL Server

D.1.1 All Databases

Please note the following general considerations with regard to database searching and indexing prior to choosing a search solution:

- You do not need to rebuild the search index when a new or custom metadata field is added.

- The base interface used for query text is a varchar2 data type. This limits text query strings to 32K. If constructing a query string to include sub-folders when searching, a system with a large number of sub-folders may cause the query string to exceed 32K and cause an error.

- If the database is used for full-text indexing, the text of each content item is stored in the database for full-text searching. It is therefore important that you size your database accordingly. Depending on the number of documents that can be indexed, the IdcColl1 and IdcColl2 tables may become very large.

- If the database is used for full-text indexing, content items are sent to the database as binary files upon check-in. The database then handles text extraction and indexing, and searches are performed using an SQL statement through the JDBC layer.

- If you want to implement full-text searching and indexing when using Sybase as the system database, you need to use one of the optional add-ons to integrate an external search solution (for example, Verity or FAST) with Content Server. You can also use these search solutions as alternatives to full-text database searching and indexing for SQL Server and Oracle.

- Database full-text does not perform zone and tokenization searching (unlike Verity).

- Accent insensitivity is available for metadata search, but not for full-text search.

- Database searching/indexing does not support PDF highlighting (unlike Verity).

- When the operator for metadata searches is set to *Matches*, Content Server searches for exact matches of a word or phrase entered into a metadata field. When search criteria is selected from an option list and that criteria contains one or more spaces, Content Server presumes the search to be a phrase and wraps the criteria in quotes.

- When doing a database search and there are more than 100,000 items in the database, some queries created from the query page will perform much better than others. You can improve performance by doing the following:

    1. Disable the calculation of the total number of items satisfying a particular search criteria (total hits) by setting the DisableTotalItemsSearchQuery equal to true in the *[CS-Install]/config/config.cfg* file as follows:

       ```
       DisableTotalItemsSearchQuery=true
       ```

    2. Ensure that all fields typically used during a search have an index on them. In particular, dSecurityGroup should have an index, and if you are using accounts, then dDocAccount should have one as well.

    3. Train users to enter values into fields that have an index on them. Use **"matches"** or "**starts with**" instead of "**substring**" when choosing the search operator.

    If you still experience performance issues, you may need a specialized component to remove the sort order functionality and restrict which queries can be performed on the query page.

D.1.2 Oracle

Please note the following considerations with database searching using Oracle:

- Content Server supports double-byte languages in Oracle 10*g*, but in Oracle 9*i* databases it supports only "space western european" (i.e., space delimited languages).

- Full-text indexing with Oracle9*i* occurs within a 60-second interval with optimization at midnight, as opposed to immediately upon check-in. (It is immediate for Oracle 10*g*). Content Server uses the Oracle CONTEXT indexing, and you can update the timing of the index. See http://www.oracle.com/technology/sample_code/products/text/index.html for more information.

- Oracle does not handle full-text indexing of XML files. Oracle attempts to transform the XML instead of reading it in as a text file.

> **Important:** For customers using Oracle database search on Oracle 10.2 databases, it is recommended that you install the latest 10.2.0.3 patchset (Patchset 5337014). The patchset is available on metalink.oracle.com.

Oracle Performance

Oracle indexes 100 GB of web pages in seven hours in Oracle 9i on a large Sun Solaris machine. Oracle's internal benchmark against the CONTEXT index indicates that the system can reach 80 queries per second, and the number of concurrent users (tests run up to 30 concurrent users) does not detrimentally affect system throughput.

In addition, to ensure that Oracle's full-text searches and regular queries perform optimally for Content Server, set optimizer_mode=FIRST_ROWS in Oracle's configuration file.

D.1.3 SQL Server

Please note the following considerations with database searching using SQL Server:

- In Content Server, the index is updated whenever the new document is updated. To change the update schedule, set UseBkgrdUpdateIndex=false in *[CS-Install]\config\config.cfg* (where *[CS-Install]* is the installation directory of the content server instance), and change the indexing update schedule as needed (in SQL Server).

D.2 Setting Up the Database for Full-Text Searching/Indexing

By default, the database used with Content Server 10*g*R3 is set up to provide metadata-only searching and indexing. Oracle and SQL Server and can be configured to also support full-text searching and indexing, in addition to metadata searching and indexing.

> **Important:** Content Server can full-text index only those languages supported for full-text indexing by the database you are using. For example, SQL 2000 does not support full-text indexing of Arabic, and so it cannot be supported in Content Server running on a SQL Server 2000 database. Check your database documentation to ensure it supports the necessary languages for your organization.

> **Tip:** Metadata-only searching provides quicker searches because less text is indexed, stored, and accessed, but it does limit the scope of search queries available to end-users.

The procedure to set up the database for full-text searching and indexing (in addition to metadata searching) depends on the database used:

- Oracle
- SQL Server

> **Note:** Sybase and DB2 do not support full-text searching and indexing. They support metadata searching and indexing only, which means nothing needs to be changed to their default Content Server 10*g*R3 configuration settings.

D.2.1 Oracle

Use the following procedure to set up Oracle for full-text searching and indexing (in addition to metadata searching/indexing):

1. Install the Content Server software and configure it to work with Oracle.

2. Add the following entry to *[CS-Install]\config\config.cfg* (where *[CS-Install]* is the installation directory of the content server instance) and save the file:

   ```
   SearchIndexerEngineName=DATABASE.FULLTEXT
   ```

3. Restart the content server.

4. **Oracle9i only:** Run the following SQL script:

   [*CS-Install*]\database\oracle\admin\fulltextindex.sql

   (where *[CS-Install]* is the installation directory of the content server instance). Make sure that you do this as the Content Server user that owns the Content Server database!

5. **Oracle10gR2 or higher only:** Run the following SQL script if you want to use search snippets in the database:

   [*CS-Install*]\database\oracle\admin\batchsnippet.sql

   (where *[CS-Install]* is the installation directory of the content server instance). Make sure that you do this as the Content Server user that owns the Content Server database!

   > **Note:** If you enabled search snippets by running this script, you can turn this feature off again by adding the following entry to Content Server's *config.cfg* file: `EnableSearchSnippet=false`.

6. Restart the content server.

7. Rebuild the search index using Repository Manager.

   > **Caution:** Rebuilding the search index may be a very time-consuming process, depending on the number of content items managed by your Content Server instance. It is therefore recommended that you perform this rebuild during off-peak hours of Content Server use (typically at night or on the weekend).

D.2.2 SQL Server

Use the following procedure to set up SQL Server for full-text searching and indexing (in addition to metadata searching/indexing):

1. Install the Content Server software and configure it to work with SQL Server.

2. Add the following entries to *[CS-Install]\config\config.cfg* (where *[CS-Install]* is the installation directory of the content server instance) and save the file:

```
SearchIndexerEngineName=DATABASE.FULLTEXT
```

3. Restart the content server.

4. Run the following SQL script, depending on the SQL Server version:

   - SQL Server 2000: [*CS-Install*]\database\ mssql2000\admin\fulltextadmin.sql

   - SQL Server 2005: [*CS-Install*]\database\ mssql\admin\fulltextadmin.sql

   (where *[CS-Install]* is the installation directory of the content server instance). Make sure that you do this as the Content Server user that owns the Content Server database.

5. Restart the content server.

6. Rebuild the search index using Repository Manager.

Caution: Rebuilding the search index may be a very time-consuming process, depending on the number of content items managed by your Content Server instance. It is therefore recommended that you perform this rebuild during off-peak hours of Content Server use (typically at night or on the weekend).

D.3 Setting Up the Database for Metadata-Only Searching/Indexing

If, after setting up the database for full-text and metadata searching and indexing, you want to revert back to metadata-only searching and indexing, complete the following steps:

1. Open the file *[CS-Install]\config\config.cfg* (where [*CS-Install*] is the installation directory of the content server instance) in a text editor.

2. Find the `SearchIndexerEngineName` parameter, and modify its value to read:

```
SearchIndexerEngineName=Database
```

3. Save the file.

4. Restart the content server.

Note: You do not need to rebuild the search index.

E

Installation Script Files

This section covers the following topics:

- "About Script Files" on page E-1
- "Script File Structure" on page E-1
- "Script File Entries" on page E-3
- "Using Script Files for Unattended Installations" on page E-10
- "Overriding Script File Entries" on page E-11
- "Performing Special Installation Tasks on the Command Line" on page E-11

E.1 About Script Files

The Content Server software is installed using script files that contain a series of installation parameters used by the installer. The parameters define, for example, where the software should be installed, what web server and database should be used, what the system locale and time zone should be, etc.

The script files are built automatically by the software installer, based on the answers provided during the sequence of installation prompts. The software is then installed using the generated script file (which is run in the background).

Content Server 10*g*R3 also supports **unattended installations**. These are basically command-line installations with a specific script file as a parameter. This enables administrators to install and set up the Content Server software on multiple computers using the exact same installation settings, without any human intervention (other than starting the installation process). For further details refer to "Using Script Files for Unattended Installations" on page E-10.

E.2 Script File Structure

Installation script files are plain-text files that can be created using any text editor such as Notepad or WordPad. They can be created from scratch, but it is recommended that you take an existing script file and modify it to suit your needs.

The easiest way to create this file is to go through a new installation of a content server all the way to the final review step. At this point, abort the installation. The installer generated an installation script file that you can use or edit. The location of the script file is *[Instance-Dir]\install*. The file name is *[date]-new.txt* or *[date]-update.txt*, where [*date*] is the current date, for example *2008-04-21-new.txt*. Please note that the date is always formatted as YYYY-MM-DD.

Parameter=Value

Each script file contains a number of installation parameters in the following format:

```
Parameter_Name=Parameter_Value
```

(where each parameter occupies one line).

Comment Lines

All lines in an installation script file that start with # are considered comment lines and are ignored. For example:

```
#This is a comment line.
```

Example

Here is an example of what a script file for a new installation could look like:

```
<?cfg jcharset="UTF8"?>
#The parameters below *must* be unique for each
#master instance across the entire enterprise.
HttpRelativeWebRoot=/master1/
IDC_Name=master1
#The parameters below *must* be unique for each
#master instance on the same computer.
TargetDir=c:/oracle/ucm/contentserver/master1/
VaultDir=c:/oracle/ucm/contentserver/master1/vault/
WeblayoutDir=c:/oracle/ucm/contentserver/master1/weblayout/
InstanceMenuLabel=Master1_Label
InstanceDescription=Content Server Master 1
DBServerDatabase=master1
IntradocServerPort=4444
IdcAdminServerPort=4440
#The parameters below do not need to be unique
#for each master instance.
InstallType=new
InstallConfiguration=Install
Platform=win32
RunChecks=true
SourceDirectory=e:/install/ecm/contentserver/win32/
InstallJvm=default
FileEncoding=UTF8
SystemLocale=English-US
UserLocale=English-US
SocketHostAddressSecurityFilter=127.0.0.1|46.68.14.*
HttpServerAddress=SCS_SERVER2
MailServer=mail.company.com
SysAdminAddress=sysadmin@mail.company.com
WebBrowserPath=c:/program files/internet explorer/iexplore.exe
WebServer=iis
DisableIISFileHandleCaching=true
NtlmSecurityEnabled=no
DatabaseType=mssql
JdbcUser=sa
JdbcPassword=idc
CreateDatabase=true
DatabaseUnicodeFields=true
Disable8dot3NameCreation=true
SearchIndexerEngineName=database
JdbcClasspath=$SharedDir/classes/jtds.jar
InstallAdminServerService=auto
InstallServerService=auto
```

E.3 Script File Entries

This section lists all installation parameters that can be included in the script files (in alphabetical order), together with descriptions, their possible values, and other considerations.

General Considerations

Please note the following general considerations:

- **Case-sensitivity**: It is recommended that you pay close attention to case when it comes to parameter values, especially for directory paths and file names. This is particularly important if script files are to be used in UNIX environments, which are case-sensitive (i.e., /u1/Oracle/ucm/contentserver/Vault is not the same as /u1/oracle/ucm/contentserver/vault). In Microsoft Windows, path and file names are not case-sensitive, which means this is not an issue there.

  Case is not important for true/false-type parameters. It does not matter if the values of such parameters are 'true', 'True', or 'TRUE'.

- **Slashes**-Make sure that you use forward slashes (/) in directory paths (for example, c:/oracle/ucm/contentserver/vault), even in a Windows environment (unless indicated otherwise).

- **Incorrect or missing parameters**: If the installer encounters invalid parameter values, the installation will typically proceed with the default values of these parameters (where possible). For example, if the value of the `CreateDatabase` parameter is set to 'nein' (rather than 'false' or 'no'), the installation will proceed, but the database tables will be created automatically (which is the default). If, however, the missing or incorrect parameter is critical for successful installation of the software, the installation is aborted. For example, if the value of the `IntradocDir` parameter (target installation directory) contains illegal characters in the path, the installation will abort since the installer has no place to copy files to.

- **Log files**: The installer creates a log file for each installation. The file is called *log.txt* and is located in the *[CS-Install]\install* directory, for example c:\oracle\ucm\contentserver\install\log.txt.

- **System variables**: You can use some system variables to refer to certain content server locations:

  - ${SourceDirectory}: This refers to the directory where the installation files for the content server software are located, for example *E:/install/UCM/ContentServer/win32* This variable can be used to make relative references to the installation directory, for example *${SourceDirectory}/../../packages/win32*.

  - $SharedDir: This refers to the location of the content server's shared files (typically the *Shared* subdirectory of the Content Server installation directory).

- **Clashing parameters**: If installation parameters clash (for example, suggesting a master installation in one and a proxied installation in another), the installation procedure is aborted.

Script File Entries

`CreateDatabase=true|yes|false|no`
This entry specifies whether the installer should attempt to create the database tables automatically. If this parameter has an invalid or no value or is not included in the script file, the database tables will be created automatically. If this parameter is set to

'false' or 'no', you need to create the database tables manually after installing the software.

`DatabaseType=mssql2000|mssql|oracle|sybase|db2|custom_database|skip_database|null_database`
This entry specifies what database will be used in conjunction with the content server. If this parameter has an invalid or no value or is not included in the script file, the database will need to be configured manually.

If you want to use DB2, or if you want to configure SQL Server, Oracle or Sybase manually, set the parameter value to `null_database`. You will then need to set up and configure the database manually after installation of the Content Server software.

`DatabaseUnicodeFields=true|yes|false|no`
This entry specifies whether Unicode text fields should be used in the database (if supported by the database). If this parameter has an invalid or no value or is not included in the script file, the database text fields will not be encoded in Unicode, but in the native database encoding. Unicode text fields in the database are generally recommended if the content server needs to handle content in Asian or bidirectional languages (for example, Japanese, Korean, Arabic, and Hebrew) or may do so in the future.

`DBServerDatabase=[name]`
This entry specifies the name of the database used in conjunction with the content server. If this parameter has an invalid or no value or is not included in the script file, the database will need to be configured manually.

Example: DBServerDatabase=db_oracle

`DBServerHost=[name]`
This entry specifies the name of the host computer running the database. If this parameter has no value or is not included in the script file, the database will need to be configured manually.

Example: DBServerHost=db_host

`DBServerPort=[port]`
This entry specifies the port number that is used to communicate with the database. If this parameter has an invalid or no value or is not included in the script file, the database will need to be configured manually.

Example: DBServerPort=1522

`Disable8dot3NameCreation=true|yes|false|no`
This entry specifies whether the 8.3 file naming convention should be disabled for the content server instance. If this parameter has an invalid or no value or is not included in the script file, the 8.3 naming convention will not be disabled.

`DisableIISFileHandleCaching=true|yes|false|no`
This entry specifies whether file handle caching for IIS should be disabled. If this parameter has an invalid or no value or is not included in the script file, it will not be disabled.

`FileEncoding=UTF8|[empty]`

This entry specifies whether UTF-8 file encoding should be used for the content server instance. If this parameter has an invalid or no value or is not included in the script file, no UTF-8 file encoding will be used, but rather the default file encoding for the specified system locale.

`HttpRelativeWebRoot=[web_root]`
This entry specifies the web server root directory as a relative URL. If this parameter has an invalid or no value or is not included in the script file, the default (/idc/) will be used. It is recommended that you only use US-ASCII characters for the parameter value. You typically access the content server login page by typing *http://[HttpServerAddress]/[HttpRelativeWebRoot]*.

Example: HttpRelativeWebRoot=/oracle/ucm/contentserver/

`HttpServerAddress=[address]`
This entry specifies the HTTP address of the web server. It is used for generating HTML pages that refer to the web server. If the web server is running on a different port than 80, make sure that you append a colon and the port number. The default is the current computer network name (if available). If this parameter has an invalid or no value or is not included in the script file, the installation is aborted. It is recommended that you only use US-ASCII characters for the parameter value.

You typically access the content server login page by typing *http://[HttpServerAddress]/[HttpRelativeWebRoot]*.

Example: HttpServerAddress=contentserver.company.com:81

`IDC_Name=[name]`
This entry specifies the unique name of the content server instance.

If you install multiple content server instances in your organization, make sure that you use different names for each of them. If this parameter has an invalid or no value or is not included in the script file, the installation is aborted.

Example: IDC_Name=SCS5

`IdcAdminServerPort=[port]`
This entry defines the port that is used to communicate with the admin server. If you install multiple master server instances on the same computer, make sure that you use different admin server ports for each of them.

Please note that proxied servers share the admin server port with their associated master content server. The default is 4440. If this parameter has an invalid or no value or is not included in the script file, the default port number will be used.

Example: IdcAdminServerPort=4440

`InstallAdminServerService=true|yes|false|no|auto`
This entry specifies how the Admin Server service should be installed. It can either be installed and started automatically ('auto'), installed but not started automatically ('true' or 'yes'), or it may not be installed altogether ('false' or 'no'). If this parameter has an invalid or no value or is not included in the script file, the service will be installed and started automatically.

`InstallerJdbcClasspath=[path]`
This entry defines the full path to the JDBC classpath that should be used with the content server instance. If this parameter has an invalid or no value or is not included

in the script file, the classpath for the standard JDBC driver for the selected database will be installed (see Chapter 3, "Pre-Installation Tasks and Considerations").

Example: InstallerJdbcClasspath=D:/Jdbc_Classpath/jtds.jar

```
InstallerJvmPath=[path]
```
This entry defines the full path to the java executable that should be used to install the Java Virtual Machine (JVM).

Example: InstallerJvmPath=D:/JVM_Installer/jdk1.5.0_11/bin/java.exe

```
InstallJvm=default|current|custom
```
This entry defines what Java virtual machine (JVM) should be installed with the content server software:

- **default:** If the parameter is set to this value, the Sun JVM 1.5 (see Chapter 3, "Pre-Installation Tasks and Considerations") will be installed for use with the content server.

- **current:** This option is relevant for updates only. If the parameter is set to this value, the JVM currently used with the (master) content server will continue to be used.

- **custom:** If the parameter is set to this value, a user-specified JVM will be used. The JvmPath parameter specifies the path to the *java.exe* executable that the content server should use.

If this parameter has an invalid or no value or is not included in the script file, the Sun JVM 1.5 (see Chapter 3, "Pre-Installation Tasks and Considerations") will be installed.

```
InstallServerService=true|yes|false|no|auto
```
This entry specifies how the content server service should be installed. It can either be installed and started automatically ('auto'), installed but not started automatically ('true' or 'yes'), or it may not be installed altogether ('false' or 'no'). If this parameter has an invalid or no value or is not included in the script file, the service will be installed and started automatically.

```
InstallServerServiceDependency=[value]
```
This entry specifies the name of a service that must run before the content server service will be started.

Example: InstallServerServiceDependency=MSSQLServer

```
InstallType=new|update|proxy
```

This entry specifies the type of installation. The following options are supported:

- **new:** This option installs a new master content server.

- **update:** This option updates an existing master content server and all its associated proxied servers.

- **proxy:** This option installs a new proxied server.

```
InstanceDescription=[description]
```
This entry specifies the long description for the content server. If this parameter has an invalid or no value or is not included in the script file, the instance description will be blank (and the installation will continue normally).

Example: InstanceDescription=Content_Server_5

`InstanceMenuLabel=[label]`

This entry specifies a short label for the content server instance. This label is used on web pages to identify this instance. The maximum number of characters for the label is 12. If this parameter has an invalid or no value or is not included in the script file, the instance description will be blank (and the installation will continue normally).

Example: InstanceMenuLabel=idc

`IntradocServerPort=[port]`

This entry specifies the port that the web server filter or any other application should use to talk to the content server instance.

If you install multiple content server instances on the same computer, make sure that you use different server ports for each of them. If this parameter has an invalid or no value or is not included in the script file, the default port number will be used. The default is 4444.

Example: IntradocServerPort=4445

`JdbcClassPath=[path]`

This entry specifies the location of the class file used for Java Database Connectivity (JDBC).

Example: JdbcClasspath=$SharedDir/classes/jtds.jar

`JdbcDriverPackageSourceFile=[file_path]`

This entry specifies the path to the JDBC driver class(es) that will be used with the content server. If you need to specify more than one file, you can separate them using semi colons: *[Path1]/[File1];[Path2]/[File2]*; etc.

Example: JdbcDriverPackageSourceFile=c:/jdbc/jdbc.jar

`JdbcDriverPackageCopy=true|yes|false|no`

This entry specifies whether the JDBC drivers from the install package specified in the JdbcDriverPackageSourceFile entry should be copied to the *[CS-Install]/shared/class* directory.

Example: JdbcDriverPackageCopy=true

`JdbcPassword=[password]`

This entry specifies the password used by the content server to access the database using Java Database Connectivity (JDBC).

Example: JdbcPassword=idc

`JdbcUser=[username]`

This entry specifies the user name used by the content server to access the database using Java Database Connectivity (JDBC).

Example: JdbcUser=oracle

`JvmPath=[path]`

This entry is used in conjunction with the `InstallJvm` parameter. It specifies the location of the custom Java virtual machine (JVM) that will be used with the content server. If this parameter has an invalid or no value or is not included in the script file, the default JVM will be used.

Example: JvmPath=c:/winnt/system32/java.exe

`MailServer=[mail_server]`
This entry specifies the name of the mail server that will be used to process content server e-mails. If this parameter has an invalid or no value or is not included in the script file, no mail server will be set.

Example: MailServer=mail.company.com

`NtlmSecurityEnabled=ntlm|adsi|no`
This entry specifies what type of security should be used:

- **ntlm:** If the parameter is set to this value, user/role/account information are mapped from Microsoft network security.

- **adsi:** If the parameter is set to this value, Active Directory Services Interface (ADSI) is used.

- **no:** If the parameter is set to this value, standard security will be used. This means that user/role/account information must be set up separately from Windows NT security.

Please note that Content Server 10*g*R3 does not support NTLM on Microsoft Windows Server 2003. If this parameter has an invalid or no value or is not included in the script file, standard security will be used.

`Platform=win32|`
This entry specifies the hardware platform that the content server software is installed on.

`RunChecks=true|yes|false|no`
This entry specifies whether the installer will perform a number of system checks before starting the installation procedure. If this parameter has an invalid or no value or is not included in the script file, the preinstallation checks will be carried out.

`RunInstall=true|yes|false|no`
If this parameter is set to 'false' or 'no', the installation procedure will not be executed. This may be useful if you want to perform the installation checks, but not go ahead with the actual installation.

`SearchIndexerEngineName=DATABASE.METADATA`
This entry specifies which search engine option should be set up for use with Content Server. The following options are supported:

- **DATABASE.METADATA:** This option sets up the content server to use the database for metadata-only searches. The content server will not have any full-text searching and indexing capability, unless you add that feature manually after the Content Server software installation.

`SocketHostAddressSecurityFilter=[IP_addresses]`
This entry specifies the incoming connection address filter, which restricts access to the content server. Only hosts with IP addresses matching the specified criteria are granted access to the content server. The default is 127.0.0.1 (localhost), but you can add any number of valid IP addresses. You can specify multiple IP addresses separated by the pipe symbol (|), and you can use wildcards (* for zero or many characters, and ? for single characters).

Example: SocketHostAddressSecurityFilter=127.0.0.1|163.192.10.*

```
SourceDirectory=[path]
```
This entry specifies the directory where the installation files of Content Server are located. If this parameter has an invalid or no value or is not included in the script file, the installation is aborted.

Example: SourceDirectory=E:/UCM/ContentServer/win32/

```
SysAdminAddress=[e-mail_address]
```
This entry specifies the e-mail address of the system administrator. If this parameter has an invalid or no value or is not included in the script file, no e-mail address will be set.

Example: SysAdminAddress=admin@company.com

```
SystemLocale=[locale]
```
This entry specifies the system locale for the content server. If this parameter has an invalid or no value or is not included in the script file, the installer will use the system locale of the operating system on the target computer.

The LocaleConfig table in *\UCM\ContentServer\resources\std_locale.htm* (lcLocaleId column) in the software distribution package lists the system locale values that can be specified.

Example: SystemLocale=English-US

```
SystemTimeZone=[time_zone]
```
This entry specifies the default time zone for the content server. If this parameter has an invalid or no value or is not included in the script file, the installer will use the current time zone of the operating system on the target computer.

The SystemTimeZones table in *\UCM\ContentServer\resources\std_locale.htm* (lcTimeZone column) on the software distribution media lists the time zone values that can be specified.

Example: SystemTimeZone=America

```
TargetDir=[path]
```
This entry specifies the installation directory of Content Server. If this parameter has no value or is not included in the script file, the installation is aborted.

Example: TargetDir=c:/oracle/ucm/contentserver/

```
UserLocale=[locale]
```
This entry specifies the default user locale for the content server. If this parameter has an invalid or no value or is not included in the script file, the installer will use the user locale of the operating system on the target computer.

The LocaleConfig table in *\UCM\ContentServer\resources\std_locale.htm* (lcLocaleId column) on the software distribution media lists the user locale values that can be specified.

Example: UserLocale=English-US

```
VaultDir=[path]
```

This entry sets the path to the root directory of the native-file repository. If this parameter has no value or is not included in the script file, the installer will assume *[IntradocDir_Variable]/vault*.

Example: VaultDir=c:/oracle/ucm/contentserver/vault

```
WebBrowserPath=[path]
```
This is the path to the web browser executable that is used to view the Content Server help system. If this parameter has an invalid or no value or is not included in the script file, Content Server's Help system will not work in the stand-alone applications.

Example: WebBrowserPath=C:/Program Files/Internet Explorer/ Iexplore.exe

```
WeblayoutDir=[path]
```
This entry sets the path to the root directory of the web-viewable file repository.If this parameter has an invalid or no value or is not included in the script file, the installer will assume *[IntradocDir_Variable]/weblayout*.

Example: WeblayoutDir=c:/oracle/ucm/contentserver/weblayout

```
WebServer=apache|nes6|iis|manual
```
This entry specifies what web server will be used in conjunction with the content server. If this parameter has an invalid or no value or is not included in the script file, the web server will need to be configured manually.

If you want to use Sun ONE, use 'nes6'.

E.4 Using Script Files for Unattended Installations

You can use script files to run unattended installations. This enables administrators to install and set up the Content Server software on multiple computers using the exact same installation settings, without any human intervention (other than starting the installation process).

> **Important:**   Before running a script file to install the Content Server software, make sure that the target computer meets all hardware and software prerequisites. For example, make sure that the web server and database specified in the script file are up and running on the target computer, that the database has been created, etc. Otherwise the installation may fail.

To perform an unattended installation, run the installer with the name of a script file as the command-line parameter, for example:

```
Installer install_script.txt
```

The installer will immediately analyze the installation script and start the installation process (providing no fatal errors were found).

For DB2 and SQL Server, when configuring script files manually, (as opposed to the auto-generated file created by the installer), you must specify the following parameters and their values when using these script files for an unattended installation:

```
JdbcDriverPackageSourceFile=[source_file_location]
JdbcDriver=[jdbc_driver]
```

E.5 Overriding Script File Entries

The installer will normally use all the installation parameters as they are included in the script file. However, it is possible to override parameter values in the script file at run time. This is done by adding one or more parameters to the command line in the following format:

```
--set-[parameter_name]=[value]
```

For example:

```
installer --set-RunChecks=false --set-InstallJvm=false script.txt
```

> **Note:** Make sure that you provide the script file name *after* any parameter overrides.

In the example above, the installer uses the file *script.txt* to obtain the installation parameters, and uses the values of the variables RunChecks and InstallJvm specified on the command line (regardless of what they are in the script file).

This may be useful in a number of situations, for example:

- Some installation parameters need to be unique for each content server instance, for example IDC_Name (i.e., instance name). You can accommodate for this by specifying this parameter on the command line.

- If a database password is required, it is stored in the script file in unencrypted form, which means that anyone who opens the text file can see the password. For security reasons, you may not want this. In that case, you can leave out the password entry in the script file and use the --set-JdbcPassword command-line parameter to provide the password at the moment you start the script file.

E.6 Performing Special Installation Tasks on the Command Line

The installer can also be used to perform a number of special installation tasks on the command line. This is done by running installer.exe with some specific parameters. You can do any of the following:

- Create or remove the configuration of IIS

- Create or remove the Content Server shortcuts from the Start menu

- Create or remove Content Server entries in the Windows Registry

- Build the portal page

To perform any of these tasks, complete the following steps:

1. Open a command prompt window and navigate to the *bin* directory of the content server that you want to perform the task for, for example *c:\oracle\ucm\contentserver\bin*.

   > **Important:** Make absolutely sure that you go to the *bin* directory of the correct content server instance. Otherwise you may unintentionally perform the installation tasks on the wrong content server instance, which may cause it to stop functioning.

2. Enter `Installer [Parameter]` and press [Enter].

3. The specified installation task is now performed.

Supported Parameters

The following parameters are supported:

`BuildPortal`

If you run the installer with this parameter, the installer rebuilds the portal page of the content server instance.

`ConfigureIIS`

If you run the installer with this parameter, the IIS web server is configured for use with the content server instance. (See also `UnconfigureIIS`.)

`CreateShortcuts`

If you run the installer with this parameter, all shortcuts for the content server instance are created in the Windows Start menu. (See also `RemoveShortcuts`.)

`Register`

If you run the installer with this parameter, all required registry entries for the content server instance are added to the Windows Registry. (See also `Unregister`.)

`RegisterAll`

If you run the installer with this parameter, the installer performs the `CreateShortCuts`, `ConfigureIIS`, and `Register` tasks in a single operation. (See also `UnregisterAll`.)

`RemoveShortcuts`

If you run the installer with this parameter, all shortcuts for the content server instance are removed from the Windows Start menu. (See also `CreateShortcuts`.)

`UnconfigureIIS`

If you run the installer with this parameter, the configuration of the IIS web server for use with the content server instance is removed. (See also `ConfigureIIS`.)

`Unregister`

If you run the installer with this parameter, all registry entries for the content server instance are removed from the Windows Registry. (See also `Register`.)

`UnregisterAll`

If you run the installer with this parameter, the installer performs the `RemoveShortCuts`, `UnconfigureIIS`, and `Unregister` tasks in a single operation. (See also `RegisterAll`.)

F

Disassociated Installations

Generally, the web server and content server are installed on the same physical computer. However, it is possible to install the content server on a different computer than the web server. This may be useful in isolated cases where enhanced security is required.

> **Note:** Because the web server is installed separately from the content server, the web server must be configured manually. For detailed instruction on manually setting up your web server after you perform these tasks, refer to Appendix A, "Setting Up Your Web Server."

This section covers the following topics:

- "Advantages and Disadvantages" on page F-1
- "Installation Procedure" on page F-2
- "Implementation Considerations" on page F-3

F.1 Advantages and Disadvantages

The main advantage of separating the web server and the content server is that this provides greater security. For example, physically separating the web server enables the web server to be placed outside of a firewall and the content server to be inside.

A completely segregated environment can be advantageous to counteract the potential risk of unauthorized access to the content server's content repository.

There are also disadvantages to using a disassociated installation:

- Reduced performance for access to files which do not need to be delivered by the Content Server Java process
- Increased complexity of installation and administration
- Lack of an automated installation
- Incomplete Oracle line of product support for this configuration (for example, Site Studio is not compatible).

> **Note:** See "Implementation Considerations" on page F-3 for some important implementation considerations.

F.2 Installation Procedure

To implement this architecture, a web server filter plug-in is available to enable you to separate the web server from the content server and retain a direct socket connection between the two servers. You must do all of the following:

- Obtaining the RedirectUrls Filter Plug-in

- Configuring Content Server

- Configuring the Web Server System

F.2.1 Obtaining the RedirectUrls Filter Plug-in

The required plug-in is named RedirectUrls.dll and is available in the *[CS-Install]\shared\os\win32\lib* directory (for example, C:\oracle\ucm\contentserver\shared\os\win32\lib). This filter plug-in allows a socket connection between the web server and content server. The filter forwards all URLs under the content server's weblayout/groups directory to be delivered by the content server.

F.2.2 Configuring Content Server

Make the following changes on the content server system:

1. Edit the *[Instance_Dir]\config\config.cfg* file to include the following lines:

   ```
   IntradocServerHostName=[Content_Server_Name]
   IdcAdminServerHostName=[Content_Server_Name]
   HttpServerAddress=[Web_Server_URL]
   SocketHostAddressSecurityFilter=[Web_Server_IP]
   ```

2. Edit the *[Instance_Dir]\admin\bin\intradoc.cfg* file to include the following line:

   ```
   SocketHostAddressSecurityFilter=[Web_Server_IP]
   ```
   (if it exists)

3. Disable the web server on the content server computer after the Content Server software has been installed and configured.

4. Restart the content server.

F.2.3 Configuring the Web Server System

Make the following changes on the web server system:

1. Create the *[Instance_Dir]* directory (for example, *C:\oracle\ucm\contentserver*).

2. Copy the following directories (the content server stub) from the content server system to this directory:

   - [*Instance_Dir*]\data

   - [*Instance_Dir*]\idcplg

   - [*Instance_Dir*]\weblayout (without the groups subdirectory)

   - [*Instance_Dir*]\shared\os\win32\lib

3. If using Microsoft IIS as your web server, you must also create the idcplg directory and set up the Virtual Directory as detailed in Appendix A of the *Oracle Universal Content Managment Content Server Installation Guide for Windows 10g Release 3 (10.1.3.3.3)*. You must copy the web filter into the IIS idcplg directory from a

Windows Oracle Content Server installation. The location of the web filter on a Windows installation is `$CS_HOME/shared/os/win32/lib`.

4. Add the RedirectUrls.dll file (see "Obtaining the RedirectUrls Filter Plug-in" on page F-2) to the newly created directory.

5. Create the [*Instance_Dir*]\data\users\SystemFilters.hda file.

6. Open the *SystemFilters.hda* file in a text editor, and add the following lines:

```
@Properties LocalData
EnableRedirectUrls=1
IntradocServerHostName=<Content_Server_Host_Name>
@end
@ResultSet IdcAuthPlugins
2
iapExportedSymbolName
iapFileNameRoot
RedirectUrls
RedirectUrls
@end
```

Note that <*Content_Server_Host_Name*> should be set to the name of your host, for example, `yourcompany.example.com`.

7. Still editing the *SystemFilters.hda* file, locate the section `@Result Set ProxiedServers` and change the value for `psIntradocServerHostName` from `localhost` to the Oracle Content Server host name.

8. Save changes and close the *SystemFilters.hda* file.

9. Create virtual directories for the web server. See Appendix A, "Setting Up Your Web Server."

10. Restart IIS.

> **Important:** Any changes to the web server configuration through Content Server will be made to the *SecurityInfo.hda* file on the Content Server system, not on the web server system. You must manually synchronize these files after any changes.

F.3 Implementation Considerations

Please note the following considerations when implementing an environment with a separate content server and web server:

- Enabling JSP
- HTTP Caching for Static Requests
- PDF Byte Streaming
- Content Server Changes Not Pushed to Web Server

F.3.1 Enabling JSP

If you want to use Java Server Pages (JSP) in a disassociated installation, where the web server and Content Server are installed on separate physical machines, you may see the following error message when trying to start a WAR file from the JSP Server Web App Admin page after enabling JSP on the content server:

```
Content Server Access Denied
```

```
Access denied to Content Server managed resource
```

When the web server is physically separated from the content server, a small portion of the Content Server directory structure (the stub) needs to be placed on the web server to enable proper operation of Content Server (see "Configuring the Web Server System" on page F-2). This structure includes the [*CS-Install*]*data**users* directory, which contains the *SecurityInfo.hda* file. This file contains role information (among several other things), as well as configuration variables specifically for JSP support. When JSP is enabled on the content server, this file is modified automatically on the physical content server. However, the version on the web server stub is not updated automatically and therefore needs to be modified manually to ensure proper JSP operation:

1. Locate the [*Instance_Dir*]\data\users\SecurityInfo.hda file within the web server stub directory, and open this file in a text editor.

2. Add the following variables to the `@Properties LocalData` section:

   ```
   IsJspServerEnabled=true
   JspEnabledGroups=jsp
   ```

   (Specify those that apply in your environment.)

3. Add the following lines to the `@ResultSet RoleDefinition` section as necessary to match your desired security configuration:

   ```
   admin
   jsp
   15
   sysmanager
   jsp
   1
   contributor
   jsp
   1
   guest
   jsp
   1
   ```

4. Save and close the file.

5. Restart the web server and the content server.

F.3.2 HTTP Caching for Static Requests

HTTP caching for static requests is not supported in disassociated installations. This means that if you have checked images into the content server to build a web site, they will be downloaded every single time, which may lead to performance issues. As a possible mitigation, you could allow the web server to read the *weblayout* directory (which is normally not allowed).

F.3.3 PDF Byte Streaming

PDF byte streaming is not supported in disassociated installations. If the web server is able to serve a PDF file directly, you can view part of that PDF file before the entire file is downloaded. This will not work if you use a disassociated web server. As a possible mitigation, you could allow the web server to read the *weblayout* directory (which is normally not allowed).

F.3.4 Content Server Changes Not Pushed to Web Server

Changes to the content server are not automatically propagated to the web server.

SecurityInfo.hda

All local user information, role definitions, and web server configurations are published from the content server to the *[Instance_Dir]/data/users/SecurityInfo.hda* file. In a disassociated web server, the content server can normally not write out to the stub directory on the web server. The *SecurityInfo.hda* file will need to be moved over manually whenever any relevant changes are made. This complicates server maintenance, but can be mitigated by using a tool like rsync to keep the files in sync.

Schema Data

When Content Server publishes the schema directory, it does so to the local *weblayout* directory. The files that the disassociated web server needs are not updated automatically. They need to be copied over manually before the changes can be seen by the users. This complicates server maintenance, but can be mitigated by using a tool like rsync to keep the files in sync.

G

Uninstalling Content Server

There are different ways to uninstall a content server instance:

- Uninstalling Content Server
- Manually Uninstalling Content Server

> **Note:** You can use either method to uninstall a content server instance, regardless of the method that was used to install that content server.

> **Important:** Do not use Add/Remove Programs in Control Panel to uninstall a proxied content server. It does not perform a complete uninstall.

G.1 Uninstalling Content Server

To uninstall a content server instance, complete the following steps:

1. Open a command prompt window and navigate to the *bin* directory of the content server that you want to uninstall, for example *c:\oracle\ucm\contentserver\bin*.

   > **Caution:** Make absolutely sure that you go to the *bin* directory of the correct content server instance. Otherwise you may unintentionally uninstall the wrong content server instance.

2. Enter `Installer UnregisterAll` and press [Enter].

3. The uninstaller now executes the following tasks:

   - It removes the content server shortcuts from the Start menu.
   - It removes the content server entries in the Windows Registry.
   - It removes the configuration of IIS (if applicable).

4. Remove the directory of the content server instance (for example *c:\oracle*\ucm\contentserver).

5. Delete the database tables used by the content server instance. It is recommended that only database administrators perform this action.

6. Remove the web server used by the content server instance. It is recommended that only system administrators perform this action.

> **Note:** After you have uninstalled the Content Server software, some shortcuts may still be in cache memory. This may cause the shortcut to be displayed, but no longer be functional. If this happens, simply log out of Windows and log back in. The shortcuts are then no longer displayed.

> **Note:** The Windows Registry of each machine running Content Server will still contain an entry HKEY_LOCAL_ MACHINE\SOFTWARE\Oracle. This registry entry was created automatically by the ISAPI filter. It is completely harmless, but may be removed if desired.

G.2 Manually Uninstalling Content Server

It is recommended that you uninstall content server instances from the command line (see "Uninstalling Content Server" on page G-1). However, there may be situations where a manual uninstallation of the Content Server software may be required. To accomplish this, complete the following steps:

> **Caution:** The procedure below removes *all* content server instances from the computer!

1. Stop all IDC services and the web server:

   a. From the **Start** menu, select **Settings**, **Control Panel**, **Administrative Tools**, and then **Services**.

   b. Stop the Content Server, Admin Server, and web server.

2. If you were using IIS, remove the ISAPI filter and delete the virtual directories:

   a. From the **Start** menu, select **Settings**, **Control Panel**, **Administrative Tools**, and then **Internet Services Manager**.

   b. Select the Default Web Site, right-click, and choose **Properties** from the popup menu.

   c. Open the ISAPI Filters tab.

   d. Select each Idc Plugin *[SCS instance name]* entry and click **Remove**.

   e. Click **OK**.

   f. Under Default Web Site, select <default web site> (i.e., oracle), right-click, and choose **Delete** from the popup menu.

   g. **(IIS 6.0 only:)** Under Web Service Extensions, Prohibit the Web Service Extension for the Idc Plugin….

3. Delete the main Content Server installation directory (for example, *C:\oracle\ucm\contentserver*).

4. Remove the Content Server group from the Start menu.

5. Empty the recycle bin.

6. Run Regedit and do the following:

    a. Delete the following registry key:

       HKEY_LOCAL_MACHINE\SOFTWARE\Oracle

    b. Delete the following registry keys for each master and proxy instance:

       HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
IdcAdminService*[Instance-Name]*_admin

       HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
IdcContentService*[Instance-Name]*

7. If you previously had MSDE installed, do the following:

    a. Stop the MSSQL Server Service.

    b. Use the Add/Remove Programs utility in Control Panel to remove the MSDE software.

8. Drop the database tables (if you are using a database other than MSDE).

9. Reboot the Content Server host machine.

Index

Symbols

${SourceDirectory} (script file entry), E-3
$SHAREDDIR (script file entry), E-3

A

ActiveDirectoryLdapComponent component, C-4
AddDefaultCharset (Apache setting), 3-6
address filter, 4-5
Admin Server
   dependent on another service, 4-12
   running as specific user, 4-11
ADSI security, 4-7
Apache
   AddDefaultCharset, 3-6
   canonical names, A-16
   debugging, A-16
   log dump file, A-16
   manual configuration, A-14
   master instances, A-14
   pre-installation tasks and considerations, 3-5
   proxied instances, A-15
Apple Macintosh
   recommended web browsers, 2-9
application
   running Content Server as an --, 7-1
ArchiverReplicationExceptions component, C-5
authentication, 4-3

B

browsers, see 'web browsers', 2-7
BuildPortal, E-12

C

canonical names
   Apache, A-16
case-sensitivity in script files, E-3
CGI directory
   Sun Web Server, A-11
CheckOutAndOpenInNative component, C-5
CheckSCSHealth component, C-6
CIS_Helper component, C-6
Classpath
   DB2, B-18

Oracle, B-8
   SQL Server, B-5
   Sybase, B-15
clustering, 1-2
command line, starting content server from --, 7-2
command-line installations
   new installations, 2-11
   new master server, 4-1
   performing specific installation tasks, E-11
   script files, E-1
   unattended installations, 4-14, E-10
   uninstalling a content server, G-1
   update installations, 2-12
   update of proxied servers, 6-6
comments in script files, E-2
components, 4-10, 6-4, C-1
   ActiveDirectoryLdapComponent, C-4
   ArchiverReplicationExceptions, C-5
   CheckOutAndOpenInNative, C-5
   CheckSCSHealth, C-6
   CIS_Helper, C-6
   ComponentTool, C-6
   ConfigMigrationUtility, C-7
   ContentAccess, C-7
   ContentFolios, C-8
   CoreUserInterfaceLibrary, C-8
   CoreWebDav, C-8
   DBSearchContainsOpSupport, C-9
   ExtendedUserAttributes, C-9
   FCKEditor, C-11
   FileStoreProvider, C-11
   Folders, C-11
   FormEditor, C-12
   installation status, C-2
   iTextComponent, C-12
   LinkManager8, C-13
   Localization, C-13
   NativeOsUtils, C-13
   OracleQueryOptimizer, C-14
   PopUpCalendar, C-14
   ProxyConnections8, C-15
   SecurityProviders, C-15
   ThreadedDiscussions, C-15
   UserProfileSchemaLoader, C-15
   WebDav, C-9
   WebUrlMapPlugin, C-16