Oracle® Content Database

Administrator's Guide

10*g* Release 1 (10.2)

B31268-02

August 2006

Oracle Content Database Administrator's Guide, 10*g* Release 1 (10.2)

B31268-02

Primary Author: Marla Azriel

Contributing Authors: Mei Hong, Alan Wiersba

Contents

1 Oracle Content DB Administration Concepts

2 Planning for Oracle Content DB Deployment

3 Oracle Content DB Security

4 Oracle Content DB Protocol Support

5 Choosing Oracle Content DB Options

6 Using Custom BPEL Workflows in Oracle Content DB

7 Managing Oracle Content DB Processes

10 Managing Oracle Content DB Formats

11 Managing Oracle Content DB Sites

12 Oracle Content DB Maintenance and Tuning

A Troubleshooting Oracle Content DB

B Migrating Content to Oracle Content DB

C Managing the Oracle Text Index

D Service Configuration Properties

E Server Configuration Properties

F FTP Quote Command Reference

G Oracle Content DB Globalization Support

Glossary

Index

Preface

Oracle Content Database (Oracle Content DB) is a consolidated, database-centric content management application that provides a comprehensive, integrated solution for file and document lifecycle management. Oracle Content DB provides both Windows and Web interfaces, and integrates with Oracle Applications E-Business Suite and other environments.

Oracle Content DB runs on Oracle Application Server and Oracle Database, and provides a scalable content management repository. Oracle Content DB also offers a comprehensive set of Web services that developers can use to build and enhance content management applications.

Audience

This document intended for system administrators, or anyone involved in configuring, running, and maintaining an Oracle Content DB instance. Oracle Content DB application administrators, such as Quota or Content Administrators, should refer to *Oracle Content Database Application Administrator's Guide* for information about application administration tasks.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see the following documents:

Oracle Content DB and Oracle Records DB

- *Oracle Content Database Application Administrator's Guide*
- *Oracle Records Database Administrator's Guide*
- *Oracle Content Database Installation Guide* for your platform
- *Oracle Content Database Release Notes* for your platform
- Oracle Content Database developer documentation

Oracle Application Server

- *Oracle Application Server Concepts*
- *Oracle Application Server Installation Guide*
- *Oracle Application Server Administrator's Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle Application Server Performance Guide*
- *Oracle HTTP Server Administrator's Guide*
- *Oracle Application Server Single Sign-On Administrator's Guide*
- *Oracle BPEL Process Manager Developer's Guide*
- *Oracle Workflow Administrator's Guide*

Oracle Enterprise Manager

- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Advanced Configuration*

Oracle Database

- *Oracle Database Administrator's Guide*
- *Oracle Database Concepts*
- *Oracle Database Advanced Security Administrator's Guide*
- *Oracle Database Performance Tuning Guide*
- *Oracle Database Backup and Recovery User's Guide*

- *Oracle Database Net Services Administrator's Guide*
- *Oracle Database Globalization Support Guide*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*
- *Oracle Text Reference*

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.

1

Oracle Content DB Administration Concepts

This chapter explains key architectural and administration concepts related to Oracle Content DB.

This chapter provides information about the following topics:

- About the Oracle Content DB System Administrator
- Oracle Content DB Architecture
- Integration with Key Oracle Technologies

About the Oracle Content DB System Administrator

Typically, Oracle Content DB **system administrators** are responsible for the following tasks:

- Planning for Oracle Content DB deployment
- Installing and configuring Oracle Content DB
- Optionally customizing Oracle Content DB by enabling **Oracle Records DB**, enabling an antivirus solution, the **FTP** and FTPS servers, retention hardware, **BFILE** archiving or aging, and other options
- Managing the Oracle Content DB **domain**, **nodes**, **services**, and **servers**
- Performing system tuning and troubleshooting
- Adding, deleting, and managing **Sites**
- Managing custom **BPEL** workflows

Note: Oracle Content DB **application administrators** are responsible for tasks related to a particular Site, such as managing users, quotas, categories, and content. There are a variety of application administration roles, such as the Category Administrator, Configuration Administrator, and Security Administrator. Users with one or more application administration roles should refer to *Oracle Content Database Application Administrator's Guide* for information about application administration tasks.

Skills Required to Administer Oracle Content DB

System administrators need to have the following skills:

- **Basic Oracle Database administration experience.** Because the file system is stored in an Oracle database, you need to understand the basics of how to administer the database, including knowledge of **Oracle Text**.
- **Knowledge of Internet and intranet protocols.** You need to understand how **HTTP**, **WebDAV**, and the other networking protocols work.
- **Oracle Application Server administration experience.** You need to understand how to administer the various components of Oracle Application Server, such as **Oracle HTTP Server**, OracleAS **Web Cache**, and Oracle Application Server Containers for J2EE (**OC4J**), using administrative tools such as the **Application Server Control**, `opmnctl`, and the **Grid Control**.

Administrative Accounts

Table 1–1 is a summary of the administrative accounts used by system administrators.

Table 1–1 Administrative Accounts

Account Name	Purpose	Notes
`ias_admin`	Used to access the Application Server Control and the Oracle Enterprise Manager 10*g* Database Control.	The password is set during **OracleAS Infrastructure** and Oracle Content DB middle-tier installation.
`sysman`	Used to access the Grid Control.	The password is set during Grid Control installation.
`orcladmin`	Used to administer a single **Oracle Identity Management** realm.	This user is the superuser for a single Oracle Identity Management **realm** and is the bootstrap user for a particular Oracle Content DB Site. For the superuser of the default realm, the password is set during OracleAS Infrastructure installation. For the superuser of any additional realms, the password is set when a realm is created. You can also use this account to access the Oracle Internet Directory Self-Service Console (`oiddas`), where you can create and manage users.
`cn=orcladmin`	Used to administer Oracle Identity Management.	This user is the superuser for Oracle Identity Management and can manage multiple realms. The password is set during OracleAS Infrastructure installation.

Oracle Content DB Administration Tools

Several administration tools are provided with Oracle Content DB, including browser-based management tools and command-line tools. Using these administration tools, you can:

- Start and stop domains and nodes
- Manage service and server objects
- Work from the command line
- Monitor domain, service, and node performance

The following sections describe the administration tools available to Oracle Content DB administrators.

Application Server Control

Oracle Enterprise Manager 10*g* Application Server Control (Application Server Control) provides access to basic Oracle Content DB process management and monitoring functions, such as starting, stopping, monitoring, and dynamically tuning the domain, nodes, services, and servers. See *Oracle Application Server Administrator's Guide* for information about how to access the Application Server Control.

Grid Control

The Oracle Enterprise Manager 10*g* Grid Control (Grid Control) is a Web-based tool that provides centralized management for Oracle Application Server middle tiers, OracleAS Infrastructure tiers, and Oracle Database hosts.

Oracle Content DB Administration Mode

Oracle Content DB **Administration Mode** provides access to application administration functions such as allocating quota and assigning roles. See *Oracle Content Database Application Administrator's Guide* for more information.

Oracle Identity Management Tools

There are several Oracle Identity Management tools you can use to manage users in Oracle Content DB:

- The Oracle Internet Directory Self-Service Console is an application that enables administrators to manage users, groups, and realms.
- Oracle Directory Manager is a Java-based tool used to manage most functions in Oracle Internet Directory. Use it to configure password policies.
- You can also use command-line tools like `ldapmodify` from the OracleAS Infrastructure tier.

See *Oracle Internet Directory Administrator's Guide* for information about the Oracle Internet Directory Self-Service Console, Oracle Directory Manager, and the Oracle Internet Directory command-line tools.

Oracle Application Server Tools

You can also use these Oracle Application Server tools:

- `opmnctl` - Manages Oracle Process Manager and Notification Server (**OPMN**). Used to start and stop Oracle Content DB, OC4J processes, Oracle HTTP Server, and OracleAS Web Cache. Can be accessed from `ORACLE_HOME/opmn/bin/`.
- `emctl` - Manages the Application Server Control. Can be accessed from `ORACLE_HOME/bin/`.

See *Oracle Process Manager and Notification Server Administrator's Guide* for more information about using the `opmnctl` tool. See *Oracle Application Server Administrator's Guide* for more information about using the `emctl` tool.

Oracle Content DB System Administration Tasks Not Covered in This Guide

Some Oracle Content DB system administration tasks are covered in other guides. The following table explains what these tasks are, and where to go for more information.

Table 1–2 System Administration Tasks and Information Not Covered in This Guide

Task	Where to Go for More Information
Installing Oracle Content DB	*Oracle Content Database Installation Guide* for your platform
Getting started after installing Oracle Content DB	*Oracle Content Database Installation Guide* for your platform
Creating and managing users	*Oracle Internet Directory Administrator's Guide*
Client certification information	Oracle*MetaLink* (`http://metalink.oracle.com`)

Oracle Content DB Architecture

The following sections describe the underlying technology for Oracle Content DB, and explain how the Oracle Content DB nodes and other processes interact. In addition, information about Oracle Internet Directory and Oracle Content DB Sites is provided.

This section contains the following topics:

- Oracle Content DB Web Services
- Oracle Content DB Application Architecture
- Oracle Content DB Domain
- Oracle Internet Directory
- The Site Model

Oracle Content DB Web Services

Oracle Content DB offers a comprehensive set of Web services that developers can use to build and enhance applications to provide sophisticated content management capabilities.

These Web services provide a large number of API calls for content and records management. The Web services also support the extensive business process automation capabilities provided by Oracle BPEL Process Manager.

Developers can use the Oracle Content DB Web services to:

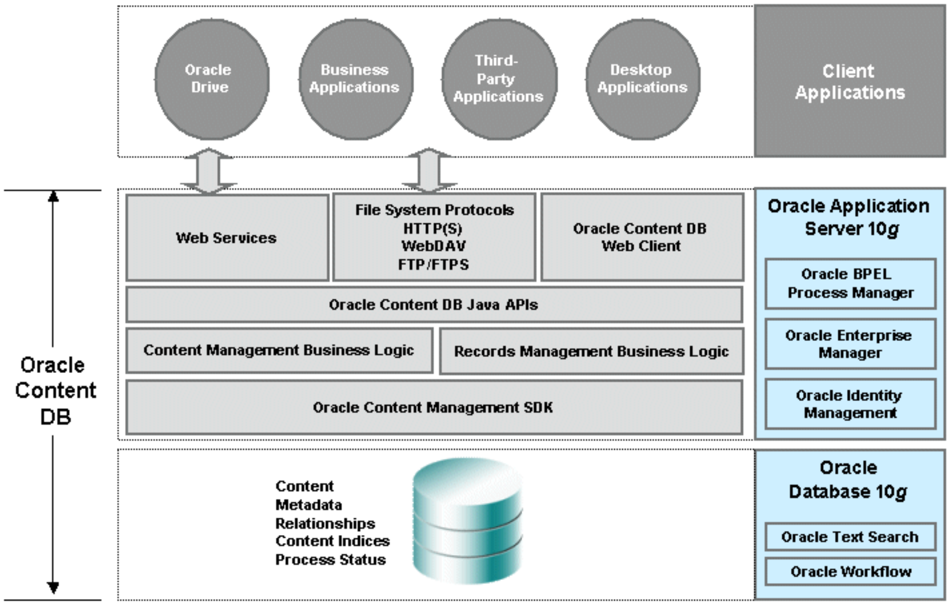
- Build custom applications that leverage Oracle Content DB to manage unstructured data
- Script and automate content-based operations
- Build custom BPEL-based workflows and use them to drive and respond to Web service invocations

See the developer documentation for more information about the Web services.

Oracle Content DB Application Architecture

A Java API layer provides a uniform interface that encompasses both content management business logic and records management business logic. This layer is the foundation for the Oracle Content DB Web application, protocol servers, and Web services. The Java API layer ensures that all components interfacing to Oracle Content DB do so at an abstraction level that respects the application business logic.

Figure 1–1 Oracle Content DB Application Architecture


Oracle Drive
Business Applications
Third-Party Applications
Desktop Applications
Client Applications
Web Services
File System Protocols HTTP(S) WebDAV FTP/FTPS
Oracle Content DB Web Client
Oracle Content DB Java APIs
Content Management Business Logic
Records Management Business Logic
Oracle Content Management SDK
Oracle Application Server 10g
Oracle BPEL Process Manager
Oracle Enterprise Manager
Oracle Identity Management
Oracle Content DB
Content
Metadata
Relationships
Content Indices
Process Status
Oracle Database 10g
Oracle Text Search
Oracle Workflow

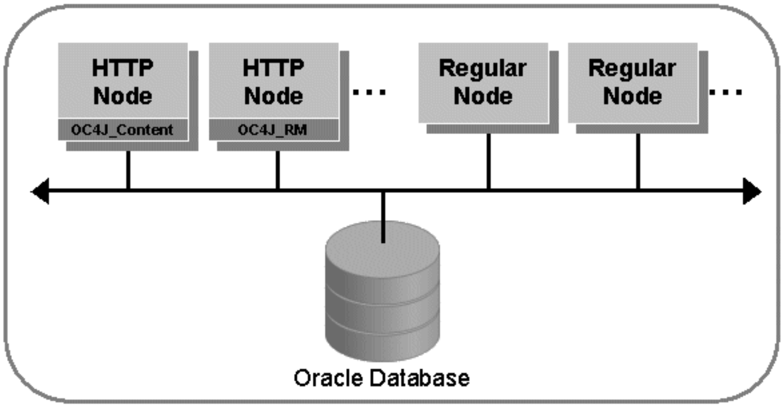
Oracle Content DB Domain

An Oracle Content DB **domain** is a logical grouping of Oracle Content DB **nodes** and an Oracle Database instance that contains the Oracle Content DB data. The nodes run on Oracle Application Server. The Oracle Content DB node processes and the database can be physically configured on a single computer or across several, separate computers.

The Oracle Content DB **schema** is created in the Oracle Content DB database during the configuration process. The schema owns all database objects, including metadata about Oracle Content DB and configuration information.

Figure 1–2 shows the Oracle Content DB domain.

Figure 1–2 The Oracle Content DB Domain



Oracle Content DB Nodes

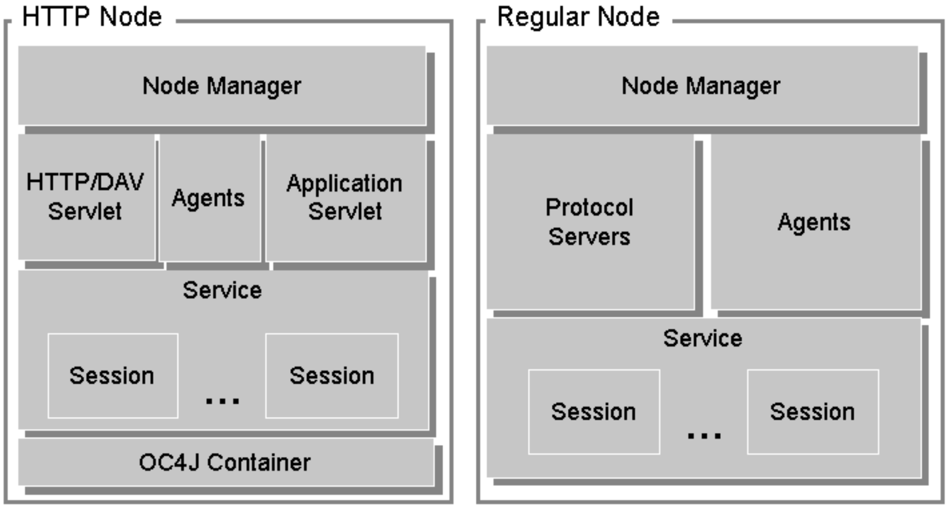
An Oracle Content DB **node** is the application software that comprises the product, along with the underlying Java Virtual Machine (JVM) required to support the software at run time.

Important concepts to understand about nodes include:

- After installation, each Oracle Content DB middle tier includes two nodes by default: one regular node and one HTTP node. (See Figure 1–3.) An additional HTTP node to support the Oracle Records DB application is also included on each middle tier, but this HTTP node and its OC4J instance are disabled by default after installation.
- The regular node supports protocol servers, such as FTP, and agents, such as the Garbage Collection Agent.
- Each regular node is monitored by OPMN, which automatically restarts the node when it is stopped unexpectedly.
- The HTTP nodes support the Oracle Content DB and Oracle Records DB applications, WebDAV, and the Web services using servlets that are configured to work with OC4J.
- The OC4J process for each HTTP node is guarded by OPMN, which restarts the OC4J process if it is stopped unexpectedly.
- The node manager is a process that is started when the node is started. It is responsible for starting the default services and servers for the node. It also provides an administrative API for the node that lets you find information about node log levels, locale information, available free memory, and the Oracle home for the node.

Figure 1–3 shows the Oracle Content DB nodes.

Figure 1–3 Oracle Content DB Nodes



Services, Servers, and Agents

Each node supports a **service** that has specific configuration parameters, such as credential managers, connections to the database, and cache sizes. By default, a single service starts on each node, and that service supports all protocol servers and agents for that node.

The **servers** supported by the service can be either protocol servers or agents. The protocol servers listen for requests from clients on a specific port and respond to requests according to the rules of the protocol specification. By default, each protocol server listens on the industry standard well-known port (for example, FTP listens on port 21) and adheres to the specification of the protocol server.

Agents perform operations periodically (time-based) or in response to events generated by other Oracle Content DB servers or processes (event-based). For example, the Content Garbage Collection Agent deletes content no longer associated with any document in Oracle Content DB. It does this based on an activation period parameter specified in the server configuration object.

Although different agents can run on different nodes, each agent must run only on a single node. Exceptions to this rule include:

- The Service Warmup Agent and the Statistics Agent must be running on all nodes, both regular and HTTP.
- The Event Handler Agent and Oracle Event Handler Agent can run on multiple nodes. See the developer documentation for more information about these agents.

Typically, most of the shipped agents must be run to ensure a stable system. See Appendix E, "Server Configuration Properties" for more information about particular agents.

The Oracle Content DB architecture is flexible: services and servers are not coupled so that you can configure services, protocol servers, and agents across a wide array of hardware. For example, you can run all protocol servers on one node, and run all agents on another node; or, they can all run on the same node.

An initial domain and node configuration is set up for you during Oracle Content DB configuration, but you can change this later. You can configure the protocol servers and other processes at any point using the Application Server Control.

See Appendix D, "Service Configuration Properties" for information about service configuration parameters. See Appendix E, "Server Configuration Properties" for information about server configuration parameters.

Oracle Internet Directory

Oracle Content DB uses Oracle Internet Directory to store and manage users.

To administer the Oracle Internet Directory associated with Oracle Content DB, use the Oracle Internet Directory Self-Service Console, Oracle Directory Manager, or other associated Oracle Internet Directory tools. See *Oracle Internet Directory Administrator's Guide* for more information.

Provisioning Users in Oracle Content DB

After users have been created in Oracle Internet Directory, they are automatically provisioned in Oracle Content DB every 15 minutes by the Oracle Internet Directory Credential Manager Agent.

You can change the default provisioning time period by changing the `IFS.SERVER.TIMER.ActivationPeriod` parameter of the Oracle Internet Directory Credential Manager Agent. You can choose a time period anywhere from 5 minutes to 24 hours. See "Modifying Server Configurations" on page 8-20 for information about changing agent parameters.

Additionally, after a user has been created in Oracle Internet Directory, signing on to Oracle Content DB as that user will immediately provision the user in Oracle Content DB, regardless of the time interval specified for the Agent. This feature, known as on-demand provisioning, can be enabled or disabled through the

`IFS.DOMAIN.CREDENTIALMANAGER.AutoUserProvisioningEnabled` domain property. See "Changing Domain Properties" on page 8-1 for more information.

Oracle Content DB and Oracle Records DB share the same provisioning model. After a user has been provisioned in Oracle Content DB, that user will be provisioned in Oracle Records DB, and the reverse. Oracle Records DB also supports on-demand provisioning.

Deleting Users

When you delete a user account in Oracle Internet Directory, the user is disabled in Oracle Content DB, and the base user information is removed from Oracle Internet Directory. Once a user account has been deleted, the only way to recover that user account is to restore a backup of Oracle Internet Directory, and then reprovision the user account in Oracle Content DB.

Because all files in Oracle Content DB reside in Libraries, users do not own content. All content belongs to the Library in which it is located. When users are deleted from Oracle Content DB, any data that was uploaded by that user remains in the Oracle Content DB repository.

In some cases, you may want to delete the Personal Library of a deleted user. To do this, you must sign on to Oracle Content DB as a user with the Library Administrator role and switch to Administration Mode. You can then navigate to the appropriate Personal Library and delete it.

The Site Model

In Oracle Content DB, a Site is a discrete organizational entity whose users can collaborate on files and folders. Users in one Site do not have access to the content of users in another Site. Oracle Content DB Sites are based on identity management realms.

During Oracle Content DB installation and configuration, a default Site is created, based on the default realm in Oracle Identity Management. You can create and manage additional Sites using the Application Server Control. See Chapter 11, "Managing Oracle Content DB Sites" for more information.

If you create more than one Site, users who are not members of the default Site must specify the corresponding realm name when they sign on to Oracle Content DB.

Each Oracle Content DB Site has a designated set of application administrators to manage quota, specify Site settings, and perform other tasks. See *Oracle Content Database Application Administrator's Guide* for more information.

Oracle Records DB shares the Oracle Content DB Site model. Each Records Administrator role is specific to a particular Site, and users of nondefault Sites must specify the realm on which their Site is based when they access Oracle Records DB.

Integration with Key Oracle Technologies

Oracle Content DB uses the capabilities of both the Oracle Database and Oracle Application Server.

This section contains the following topics:

- Integration with Oracle Database
- Integration with Oracle Application Server

Integration with Oracle Database

Oracle Content DB uses Oracle Database to store all content and metadata.

Oracle Database and the Oracle Content DB Schema

All content and metadata about the Oracle Content DB instance is stored in an Oracle database. These objects, including tablespaces, tables, indexes, views, sequences, and procedures owned by the schema, provide the underpinnings of a fully functioning system.

There are additional schemas created to ensure secure connectivity to other systems. These additional schema names are derived from the Oracle Content DB schema name. For example, if the Oracle Content DB schema name is `CONTENT`, the additional schemas are `CONTENT$CM` and `CONTENT$ID`.

User content, such as word processing files, spreadsheets, sound files, and presentations, is stored by Oracle Content DB in the database as large objects (LOBs).

LOBs enable fast access and optimized storage for large bits of content, often binary, stored in the database. Otherwise, all content in the Oracle Content DB schema is stored as standard data types in various tables.

Oracle Text

Oracle Text is full-text retrieval technology built into Oracle Database for indexing and searching text and documents. Oracle Text supports mixed languages and character sets in the same index. Oracle Content DB uses the text indexing and retrieval features of Oracle Text.

Oracle Streams Advanced Queueing

Oracle Streams Advanced Queueing provides an infrastructure for distributed applications to communicate asynchronously using messages. Oracle Streams Advanced Queueing is built into Oracle Database.

Oracle Content DB uses Oracle Streams Advanced Queueing to integrate with Oracle Workflow and Oracle BPEL Process Manager.

Oracle Real Application Clusters (Oracle RAC)

A cluster is a group of computers that work together and behave as a single system. Clustering requires both hardware (interconnect) and software (clusterware) support. In the past, clusters were used in high availability read-only applications, such as data warehouses. Now, clusters are increasingly becoming a lower-cost approach for computing applications that require high availability and scalability.

An Oracle Real Application Cluster consists of two or more computers configured to interact and provide the appearance of a single Oracle database. These Oracle RAC nodes are linked by an interconnect. The interconnect serves as the communication path between each node in the cluster database. Each Oracle Database instance uses the interconnect for the messaging that synchronizes each instance's use of shared resources. Oracle also uses the interconnect to transmit data blocks that are shared by the multiple instances. The data files accessed by all the nodes are the primary type of shared resource.

Oracle RAC requires that all nodes have simultaneous access to the shared disks to give the instances concurrent access to the database. The implementation of the shared disk subsystem is based on your operating system: you can use either a cluster file system, or place the files on raw devices. Cluster file systems simplify the installation and administration of Oracle Real Application Clusters.

When you add or remove Oracle RAC nodes for Oracle Content DB, the Oracle RAC databases are automatically registered in Oracle Internet Directory. Oracle Content DB uses the information stored in Oracle Internet Directory to connect. Although you do not need to specify database connection information on middle tiers, you must restart the Oracle Content DB domain after you add or remove an Oracle RAC node.

For more information about Oracle RAC, see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*.

Integration with Oracle Application Server

Oracle Content DB is designed to integrate with several components from the Oracle Application Server product family, including Oracle Internet Directory, the Application Server Control, and OC4J.

Oracle Application Server Containers for J2EE (OC4J)

OC4J is a J2EE-compliant application server that supports Java Server Pages (JSP), Java servlets, and many other APIs from the Java 2 Platform, Enterprise Edition (J2EE). Services are deployed to an OC4J instance using XML-based configuration files as standard Web Application Archive(.WAR), Enterprise Application Archive (.EAR), Resource Adapter Archive (.RAR), and Java Archive (.JAR) files. Oracle Content DB uses the Java Servlet and the run-time environment of OC4J to support the HTTP/DAV servlet, application servlet, and Web services.

OC4J is automatically configured for the Oracle Content DB HTTP node and the Oracle Records DB HTTP node as part of the Oracle Content DB configuration process. You can manage OC4J through the Application Server Control.

Oracle Process Manager and Notification Server (OPMN)

OPMN manages all the components within an application server instance, including Oracle HTTP Server, OC4J processes, and OracleAS Web Cache. It channels all events from different components to all components interested in receiving them.

OPMN provides the following functionality:

- Provides a command-line interface for process control and monitoring for single or multiple Oracle Application Server components and instances.
- Provides an integrated way to manage Oracle Application Server components.
- Solves interdependency issues between Oracle Application Server components by enabling you to start and stop components in order.
- Provides automatic restart of Oracle Application Server processes when they become unresponsive, terminate unexpectedly, or become unreachable as determined by ping and notification operations.

The OPMN server should be started as soon as possible after turning on the computer. OPMN must be running whenever OPMN-managed components are turned on or off.

Note: On the Microsoft Windows operating system, OPMN is installed as a Windows service (`Oracle<OracleHomename>ProcessManager`). It starts up automatically when you start or restart your computer.

You can use the OPMN command-line tool, `opmnctl`, to manage Oracle Content DB. For complete information about `opmnctl` syntax and usage, see *Oracle Process Manager and Notification Server Administrator's Guide*.

Oracle Enterprise Manager

Oracle Enterprise Manager is a systems management software application that enables you to manage and monitor Oracle Application Server instances and other Oracle products. You can use the following Oracle Enterprise Manager Web-based interfaces:

- Use the Oracle Enterprise Manager 10*g* Application Server Control (Application Server Control) to manage Oracle Content DB middle-tier hosts and OracleAS Infrastructure hosts.

  Use the Application Server Control to operate and monitor system processes associated with the Oracle Content DB domain and nodes.

- Use the Oracle Enterprise Manager 10*g* Grid Control (Grid Control) for centralized management of Oracle Application Server middle tiers, OracleAS Infrastructure tiers, and Oracle Database hosts.

  If you want to use the centralized management capabilities of the Grid Control, you must install and configure the Grid Control. You must also install a separate Management Agent on each Oracle Content DB middle-tier computer in its own Oracle home. For more information, refer to *Oracle Enterprise Manager Concepts*.

You can access the Application Server Control using a Web browser from anywhere on the network. The first page you see is the Oracle Application Server Farm Home page, which lets you view the application server instances in your Oracle Content DB deployment. From this page, you can access the Application Server Home page, which shows the Oracle Application Server components configured for the current middle tier.

Use the Grid Control for access to Oracle Content DB metrics, such as document statistics, node statistics, and users, including access to historical metric data. The Grid Control is also used for monitoring system health through alerts that have been defined for some metrics.

Oracle Internet Directory

Oracle Internet Directory is a Lightweight Directory Access Protocol (LDAP) v.3-compliant directory service implementation. Oracle Internet Directory provides user authentication and other directory service features, such as user provisioning, to Oracle Content DB. See *Oracle Internet Directory Administrator's Guide* for more information.

Oracle BPEL Process Manager

Oracle BPEL Process Manager provides a framework to design, deploy, monitor, and administer processes based on BPEL standards. You can define custom BPEL workflows in Oracle BPEL Process Manager, and then register them for use in Oracle Content DB. Custom workflows are only available to the default Site in Oracle Content DB; additional Sites cannot use the custom workflows. See Chapter 6, "Using Custom BPEL Workflows in Oracle Content DB" for detailed information.

About BPEL The Business Process Execution Language (BPEL) is an XML-based language for enabling task-sharing across multiple enterprises using a combination of Web services. BPEL is based on the XML schema, Simple Object Access Protocol (SOAP), and Web Services Description Language (WSDL). Using BPEL, you design a business process that integrates a series of discrete services into an end-to-end process flow. For more information about BPEL and Oracle BPEL Process Manager, see *Oracle BPEL Process Manager Developer's Guide*.

Oracle Workflow

Oracle Workflow is business-process automation software. You can use Oracle Workflow to automate the process of routing and approving information, according to business rules you specify. Oracle Content DB integrates with Oracle Workflow to support the default workflow processes shipped with Oracle Content DB.

You can view workflow notifications by accessing the Oracle Content DB Reports feature, or you can configure Oracle Workflow to send e-mail notifications. See Chapter 6, "Using Custom BPEL Workflows in Oracle Content DB" for more information.

2

Planning for Oracle Content DB Deployment

This chapter explains how to plan for an Oracle Content DB deployment.

This chapter provides information about the following topics:

- Oracle Content DB Deployment Configurations
- Oracle Content DB Sizing Guidelines
- Oracle Content DB Tablespaces

Oracle Content DB Deployment Configurations

This section describes the two types of Oracle Content DB deployment and provides information about high availability considerations.

This section contains the following topics:

- Single-Computer Deployment
- Multiple-Computer Deployment
- High Availability Considerations

Single-Computer Deployment

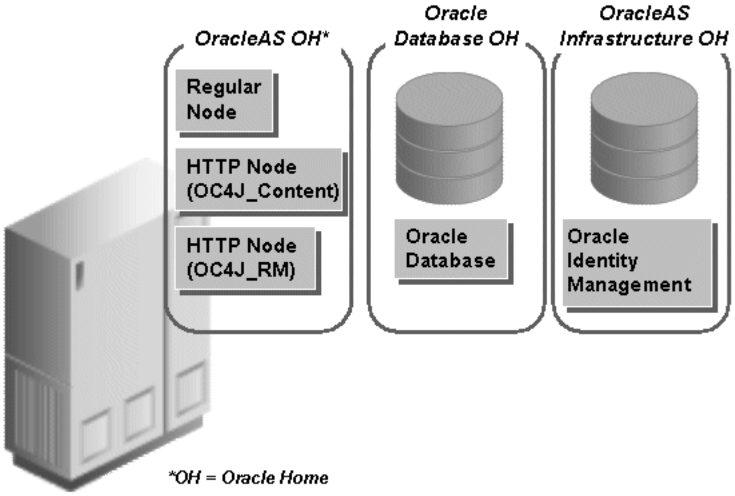
Oracle Content DB can be installed on a single computer if the computer meets the recommended hardware and software requirements. If your computer does not meet the recommended requirements, the performance of this configuration might be less than satisfactory. See *Oracle Content Database Installation Guide* for your platform for more information about hardware and software requirements.

In a single-computer deployment, Oracle Content DB and all required components are installed on a single computer. These components include Oracle Identity Management and Oracle Database. A single-computer deployment does not allow you to use load balancing or failover options.

Because Oracle Content DB uses Oracle Internet Directory for credential management, the computer typically requires at least three Oracle homes: one for Oracle Database, one for OracleAS Infrastructure, and one for the Oracle Content DB middle tier. See "Oracle Content DB Sizing Guidelines" on page 2-3 for information about the number of supported users for single-computer deployment.

Figure 2–1 shows an Oracle Content DB domain running on a single computer.

Figure 2–1 Single-Computer Oracle Content DB Deployment



See "Oracle Content DB Nodes" on page 1-5 for more information about the Oracle Content DB processes shown in Figure 2–1.

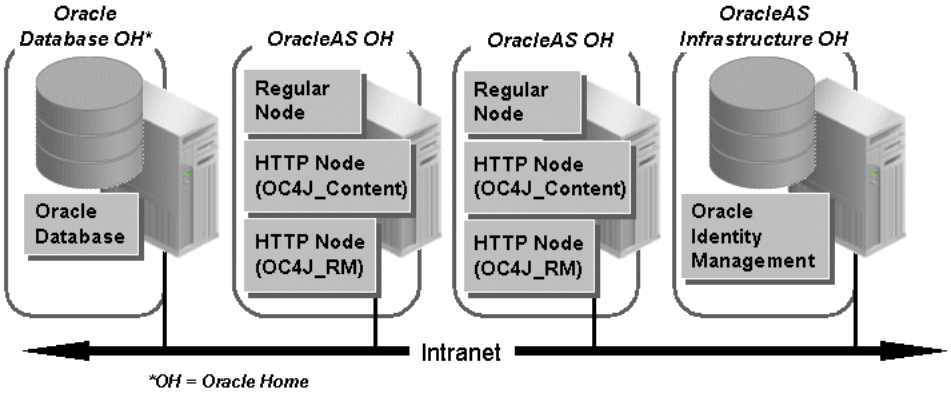
Multiple-Computer Deployment

Oracle Content DB can be deployed on multiple computers. This configuration enables you to separate the components, and configure failover, load balancers, and high availability options. With multiple-computer deployment, you can also use computers with lower hardware requirements than required for single-computer deployment. See *Oracle Content Database Installation Guide* for your platform for more information about hardware requirements.

With the appropriate network load balancers and computer configuration, users may not know whether the Oracle Content DB instance is running on one host or across several hosts. Users access content, such as folders and files, using the appropriate client application for a particular Oracle Content DB protocol server.

Figure 2–2 is an example of a multiple-computer deployment, with Oracle Content DB components distributed across four computers.

Figure 2–2 A Multiple-Computer Oracle Content DB Deployment



See "Oracle Content DB Nodes" on page 1-5 for more information about the Oracle Content DB processes shown in Figure 2–2.

Each Oracle Content DB middle tier can include HTTP nodes, regular nodes, or both. Most Oracle Content DB agents can only run on one middle tier at a time. However, agents can be deployed on multiple middle tiers in an inactive state, and activated if the middle tier on which they were running fails. See the following section for more information.

High Availability Considerations

When you first configure Oracle Content DB, the first middle tier that you configure contains important configuration settings that are not stored in subsequent middle tiers. Because of this, if you choose to deinstall the first Oracle Content DB middle tier, or if the first middle tier goes down, you must ensure these configuration settings are restored on another middle tier.

The following list is a summary of these configuration settings:

- If you were running some or all of the Oracle Content DB agents on a particular middle tier that is deinstalled or becomes unavailable, you must configure these agents to run elsewhere. To do this, modify the node configuration of a node running on another Oracle Content DB middle tier. See "Modifying Node Configurations" on page 8-8 for more information.
- The `IFS.DOMAIN.APPLICATION.ApplicationHost` domain property points to a particular middle tier (typically the first that was configured). If that middle tier is deinstalled or becomes unavailable, you must update this domain property to point to another Oracle Content DB middle tier. See "Changing Domain Properties" on page 8-1 for more information.
- If you were using Oracle Mail as your SMTP server, and you were running Oracle Mail on a particular middle tier that is deinstalled or becomes unavailable, you must update the `IFS.DOMAIN.EMAIL.SmtpHost` and `IFS.DOMAIN.EMAIL.SmtpPort` domain properties to point to another SMTP server. See "Changing Domain Properties" on page 8-1 for more information.
- If you collected domain and repository metrics on a particular middle tier that is deinstalled or becomes unavailable, you must configure these metrics on another Oracle Content DB middle tier. See "Configuring Performance Metrics" on page 9-4 for more information.

Oracle Content DB Sizing Guidelines

This section describes hardware requirements for a sample deployment of Oracle Content DB and formulas that allow you to determine the hardware configuration required to deploy Oracle Content DB in your organization.

This section includes the following topics:

- Hardware Requirements
- Sizing Formulas for Each Middle-Tier Computer
- Sizing Formulas for the Database Computer
- Memory Requirements: Sample Deployment

Hardware Requirements

Hardware requirements for Oracle Content DB are primarily determined by the factors described in Table 2–1.

Table 2–1 Primary Factors Determining Oracle Content DB Hardware Requirements

Hardware Resource	Middle-tier computer requirement variables	Database computer requirement variables
CPU	■ Peak number of operations performed each second	■ Peak number of operations performed each second ■ Whether using Oracle Text indexing
Memory	■ Peak number of operations performed each second ■ Peak number of concurrent connected users ■ Average number of protocols used each concurrent connected user ■ Average number of sessions used each concurrent connected user ■ Number of users accessing Oracle Content DB through FTP ■ Number of files each folder	■ Peak number of operations performed each second ■ Number of files
Disk Size	Not applicable	■ Number of files ■ Average content size of files, whether they can be indexed or not
Disk Throughput	Not applicable	■ Peak number of files read and written each second ■ Average content size of files

In order to determine hardware requirements, assumptions must be made about the type of work that users are performing. The following measurements are averages extrapolated from the deployment of Oracle Content DB within Oracle Corporation (40,000+ users), and are generally applicable for projecting Oracle Content DB usage.

Table 2–2 User Profiles

User Task	Number of Operations Each Connected User Performs Each Hour
Folder opens	8
Files read or written	10
Queries	0.1

These sizing guidelines are based on benchmarks of 10,000 concurrent connected users on Sun Microsystems hardware. The guidelines have been validated against measurements taken from internal Oracle Corporation production usage of Oracle Content DB by 55,000 Oracle employees, with 30 million files and 13TB of content. This system uses Intel Linux hardware for the middle-tier computers, and Sun hardware for the database.

Note: The sizing guidelines discussed in the following sections may be inaccurate if the desired user profile is significantly larger than the average measurements detailed in Table 2–2.

Sizing Formulas for Each Middle-Tier Computer

This section provides formulas that you can use to determine specific hardware sizing for each middle-tier computer. Table 2–3 summarizes the sizing formulas.

Table 2–3 Oracle Content DB Sizing Recommendations for Each Middle-Tier Computer

Component	Sizing Recommendations
Number of CPUs	`roundup(`*`peak concurrent connected users`*` / 250 + 33% headroom)`
Required Usable Disk Space	At least 500MB for Oracle Content DB
Total Computer Memory, HTTP as the Primary Protocol	If HTTP is the primary protocol: `480MB + (3.6 MB * `*`peak concurrent connected users`*`)`
Total Computer Memory, Primary Protocol Other Than HTTP	If HTTP is not the primary protocol, or if the desired user profile is different than the average measurements described in Table 2–2: `480MB + (1MB * `*`peak concurrent connected users`*` * `*`average number of sessions in use by each concurrent connected user`*`) + (3KB * `*`number of objects desired in the java object cache`*`) + (8MB * `*`number of connections to the database`*`)`

Number of CPUs

Use the following formula to determine the number of CPUs required:

```
roundup(peak concurrent connected users / 250 + 33% headroom)
```

The `peak concurrent connected users` parameter is the number of users who are signed in to Oracle Content DB and have performed an operation during the peak hour of the day. If you do not know how many users that is likely to be, assume 10% of your entire Oracle Content DB named user population.

The `headroom` parameter represents the amount of CPU resources that should be left available. In order to ensure optimal efficiency, no more than 75% of the CPU should be allocated.

This formula is based on the following assumptions:

- The formula assumes Sun SPARC Solaris 400MHz UltraSPARC-II processors with 8MB secondary cache.
- Other RISC processors should perform roughly proportional to their MHz.
- Intel Pentium III (or later) processors on Windows and Linux computers should perform roughly proportional to half their MHz. For example, an 800MHz Pentium processor is approximately equivalent to a 400MHz RISC processor.

Required Usable Disk Space

Allocate at least 500MB for Oracle Content DB.

Total Computer Memory, HTTP as the Primary Protocol

If HTTP is the primary protocol, use the following formula to determine the total computer memory required:

```
480MB + (3.6MB * peak concurrent connected users)
```

The 480MB is for the first Oracle Content DB middle-tier computer. The value of 3.6MB is calculated from the following assumptions:

- **1.6 sessions per concurrent connected user**: This assumes that the primary interface for Oracle Content DB is through the HTTP node. The additional 0.6 sessions are HTTP sessions which are started whenever a user of the Oracle Content DB Web client starts another Oracle Content DB Web client, or if the user accesses Web Folders or Oracle Drive.
- **0.1 connection pool connections per concurrent connected users**: This assumes the stated user profile.
- **400 objects in the Java data cache per concurrent connected user**: This assumes 50 files per folder and 8 folders opened per hour, assuming the stated user profile.

Total Computer Memory, Primary Protocol Other Than HTTP

If HTTP is not the primary protocol, or if the desired user profile is different than the average measurements described in Table 2–2, use the following formula to determine the total computer memory required:

```
480MB + (1MB * peak concurrent connected users * average number of sessions in use
by each concurrent connected user) + (3KB * number of objects desired in the Java
object cache) + (8MB * number of connections to the database)
```

The 480MB is for the first Oracle Content DB middle-tier computer. The other values are calculated from the following assumptions:

- The value of 1MB is high by design. Oracle Content DB has been optimized to reduce database CPU load by using middle-tier memory to cache items. This ensures a more scalable and less expensive system, because the database computer is less of a scalability bottleneck, and because memory on one- or two-processor middle-tier computers is typically less expensive than memory or CPU on high-end database computers (computers with large amounts of attached storage or with many processors).
- Oracle recommends limiting the number of peak concurrent user sessions through the `IFS.SERVICE.MaximumConcurrentSessions` parameter in the service configuration. Oracle has tested with Java heaps up to 2GB. With this constraint, this implies up to approximately 700 concurrent connected users per node and a total of 1986MB in size, if the following are true:
  - Each user uses 1.6 sessions
  - Each session is 1MB (700 * 1.6 * 1MB = 1,120MB)
  - Each user needs 400 Java data cache objects
  - Each object is 3KB in size (700 * 400 * 3KB = 866MB)

  For each additional node on the same computer, you must include the node overhead in the sizing. See Table 2–5 for more information.

  The HTTP/WebDAV memory overhead includes memory for 10 simultaneous guest user requests. Because of this, guest users should not be counted as connected users for HTTP/WebDAV access.
- For the average number of sessions in use by each concurrent connected user, use the value 1.6 for the HTTP node.
- Calculate the number of objects desired in the Java object cache by using the following formula:

  ```
  (number of folder opens in the peak hour) * (number of objects per folder) *
  ```

`(number peak concurrent connected users)`

Use the result to set the value of the `IFS.SERVICE.DATACACHE.Size` parameter.

- The number of connections to the database depends on the number of simultaneous read or write operations being performed. Assume 0.1 database connections per user if using a standard user profile. This is a sum of the parameters `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSize` and `IFS.SERVICE.CONNECTIONPOOL.READONLY.MaximumSize` for each service.

See "Service Configurations and Java Memory Sizing" on page 12-1 for more information on middle-tier memory.

Sizing Formulas for the Database Computer

This section provides formulas that you can use to determine specific hardware sizing for each database computer to be used for Oracle Content DB users. Table 2–4 summarizes the sizing formulas.

Table 2–4 Oracle Content DB Sizing Recommendations for the Database Computer

Component	Sizing Recommendations
Number of CPUs	`roundup(`*`peak concurrent connected users`*` / 250 + 33% headroom)`
Required Usable Disk Space	`4.5GB + `*`total raw file size`*` + (`*`total raw files size`*` * 20%)`
Total Computer Memory	`64MB + 128MB + `*`database buffer cache`*` + (1MB * `*`number of connections to the database`*`) + (500 bytes * `*`number of files`*`) + (100KB * `*`peak concurrent connected users`*`)`

Number of CPUs

Use the following formula to determine the number of CPUs required:

```
roundup(peak concurrent connected users / 250 + 33% headroom)
```

The *`peak concurrent connected users`* parameter is the number of users who are signed in to Oracle Content DB and have performed an operation during the peak hour of the day. If you do not know how many users that is likely to be, assume 10% of your entire Oracle Content DB named user population.

The *`headroom`* parameter represents the amount of CPU resources that should be left available. In order to ensure optimal efficiency, no more than 75% of the CPU should be allocated. One additional CPU is used for the background Oracle Text indexing of new file content, if you are using Oracle Text indexing.

This formula is based on the following assumptions:

- The formula assumes Sun SPARC Solaris 400MHz UltraSPARC-II processors with 8MB secondary cache.
- Other RISC processors should perform roughly proportional to their MHz.
- Intel Pentium III (or later) processors on Windows and Linux computers should perform roughly proportional to half their MHz. For example, an 800MHz Pentium processor is approximately equivalent to a 400MHz RISC processor.

Required Usable Disk Space

Use the following formula to determine the usable disk space required:

```
4.5GB + total raw file size + (total raw file size * 20%)
```

The 4.5GB represents the space required for Oracle software and the initial database configuration. If you are not using Oracle Text to index the content, multiply the total raw file size by 15% instead of 20%.

The following considerations can increase the amount of usable disk space required for the database computer:

- Mirroring for backup and reliability
- Redo log size, which should be determined by how many files are inserted and their size
- Unused portion of the last extent in each database, which occurs with pre-created database files or which can be large if the next extent setting is large

Total Computer Memory

Use the following formula to determine the total computer memory required:

```
64MB + 128MB + database buffer cache + (1MB * number of connections to the
database) + (500 bytes * number of files) + (100KB * peak concurrent connected
users)
```

This formula is based on the following assumptions:

- 128MB is the minimum amount of memory required to run a small Oracle Server.
- Number of files: The database buffer cache in the default Oracle database configuration is sufficient for approximately 50,000 files. For deployments with more than 50,000 files, allocate 500 bytes per file for optimal performance, including wildcard filename searches. Reduce this number if users do not perform wildcard filename searches.
- 100KB is calculated by assuming that 0.1 database connections are needed per concurrent connected user as in the stated user profile. Each database connection takes approximately 1MB of database memory.

Memory Requirements: Sample Deployment

Table 2–5 describes approximate minimum memory overhead on the middle-tier computers for each component.

Table 2–5 Memory Overhead by Component

Description	**Approx. minimum memory (MB) for middle-tier computer running a regular node and HTTP node**	**Approx. minimum memory (MB) for middle-tier computer running an additional HTTP node**	**Approx. minimum memory (MB) for middle-tier computer running an additional regular node**
Memory used by the operating system upon booting the computer.	60	60	60
Overhead for first Java Virtual Computer (JVM).	30	30	30

Table 2–5 (Cont.) Memory Overhead by Component

Description	Approx. minimum memory (MB) for middle-tier computer running a regular node and HTTP node	Approx. minimum memory (MB) for middle-tier computer running an additional HTTP node	Approx. minimum memory (MB) for middle-tier computer running an additional regular node
Application Server Control. Must run on every middle tier.	150	150	150
Regular Oracle Content DB node JVM. Typically runs the FTP server (if you enable FTP) and the Oracle Content DB agents.	50	0	50
Oracle HTTP Server, including the default HTTP daemons. Required for Oracle Content DB Web client, HTTP, Web Folders, and Oracle Drive access.	30	30	0
Oracle Content DB OC4J process. Required for Oracle Content DB Web client, HTTP, Web Folders, and Oracle Drive access. Must be paired with Oracle HTTP Server.	130	130	0
Total	**450**	**400**	**290**

Oracle Content DB Tablespaces

This section provides information about the Oracle Content DB tablespaces, and includes the following topics:

- Data Types and Storage Requirements
- Storing Files in an Oracle Database
- Oracle Content DB Metadata and Infrastructure
- Oracle Text
- Disk Space Requirements: Sample Deployment

Data Types and Storage Requirements

Table 2–6 shows the different types of data stored in Oracle Content DB and describes the purpose of each tablespace. Each of these tablespaces will be discussed in further detail in subsequent sections of this file.

Table 2–6 Tablespace Definitions

Tablespace Type	Tablespace Name	Description
File Storage	`CONTENT_IFS_LOB_I`	Stores the Large Object (LOB) data for files that are indexable by Oracle Text, such as text and word processing files.
File Storage	`CONTENT_IFS_LOB_N`	Stores the LOB data for files that are not indexed by Oracle Text, such as zip files.
File Storage	`CONTENT_IFS_LOB_M`	Stores the LOB data for files that are indexable by Oracle *inter*Media, such as image, audio, and video files.
Oracle Text	`CONTENT_IFS_CTX_I`	Stores words (tokens) extracted by Oracle Text from Oracle Content DB files (the Oracle table `DR$IFS_TEXT$I`).
Oracle Text	`CONTENT_IFS_CTX_X`	Stores the Oracle B*tree index on the Oracle Text tokens (the Oracle index `DR$IFS_TEXT$X`).
Oracle Text	`CONTENT_IFS_CTX_K`	Stores miscellaneous Oracle Text tables (the Oracle tables `DR$IFS_TEXT$K`, `DR$IFS_TEXT$N`, `DR$IFS_TEXT$R`).
Metadata	`CONTENT_IFS_MAIN`	Stores metadata for files, information about users and groups, and other Oracle Content DB object data.
Oracle Workflow	`WORKFLOW_IFS_MAIN`	Stores data for Oracle Workflow.
General Oracle Storage	Various	`SYSTEM`, `ROLLBACK`, `TEMP`, and other tablespaces that store the Oracle data dictionary, temporary data during transactions, and so on.

Typical tablespace storage space and disk I/O are detailed in Table 2–7:

Table 2–7 Tablespace Storage Requirements and Disk I/O

Tablespace	% of Total I/O Throughput Requirements	% of Disk Space Requirements
`CONTENT_IFS_MAIN`	50%	2%
`CONTENT_IFS_CTX_X`	20%	1%
`CONTENT_IFS_CTX_I`	10%	1%
`CONTENT_IFS_LOB_I`	8%	35%
`CONTENT_IFS_LOB_N`	5%	55%
Various	5%	1%
`CONTENT_IFS_LOB_M`	1%	4%
`CONTENT_FS_CTX_K`	1%	1%
Total	**100%**	**100**

Note the following issues regarding the information in Table 2–7:

- I/O rates are highly dependent on the size of the `db_cache_size`. These measurements were taken on the Oracle-internal Oracle Content DB implementation, with 8GB `db_cache_size`, 17 million files, and 40,000 named users.

- The `CONTENT_IFS_MAIN` tablespace is the most important tablespace to spread across disks for maximum I/O capacity.
- Disk I/O for the `CONTENT_IFS_CTX_I`, `CONTENT_IFS_CTX_X` and `CONTENT_IFS_CTX_K` tablespaces is largely generated from Oracle Text batch processes (`ctx_ddl.sync_index`, and `ctx_ddl.optimize_index`), which are not critical to end-user performance. Therefore, these tablespaces can be on disks with lower I/O capacity, if necessary.

Storing Files in an Oracle Database

The largest consumption of disk space will occur on the disks that actually contain the files that reside within Oracle Content DB, namely the `CONTENT_IFS_LOB_I` tablespaces, `CONTENT_IFS_LOB_N` tablespaces, and `CONTENT_IFS_LOB_M` tablespaces. This section explains how the files are stored and how to calculate the amount of space those files will require.

As previously mentioned, files stored in Oracle Content DB are actually stored in database tablespaces. Oracle Content DB makes use of the Large Object (LOB) facility of the Oracle Database. All files are stored as Binary Large Objects (BLOBs), which is one type of LOB provided by the database. LOBs provide for transactional semantics much like the normal data stored in a database. In order to accomplish these semantics, LOBs must be broken down into smaller pieces which are individually modifiable and recoverable. These smaller pieces are referred to as chunks. Chunks are a group of one or more sequential database blocks from a tablespace that contains a LOB column.

Both database blocks and chunk information within those blocks (BlockOverhead) impose some amount of overhead for the stored data. BlockOverhead is presently 60 bytes per block, which consists of the block header, the LOB header, and the block checksum. Oracle Content DB configures its LOBs to have a 32K chunk size.

As an example, assume that the `DB_BLOCK_SIZE` parameter of the database is set to 8192(8K). A chunk would require four contiguous blocks and impose an overhead of 240 bytes. The usable space within a chunk would be 32768-240=32528 bytes.

Each file stored in Oracle Content DB consists of an integral number of chunks. Using the previous example, for instance, a 500K file will actually use 512000/32528=15.74=16 chunks. Sixteen chunks will take up 16*32K = 524288 bytes. The chunking overhead for storing this file would then be 524288-512000=12288 bytes which is 2.4 percent of the original file’s size.

The chunk size used by Oracle Content DB is set to optimize access times for files. Note that small files, files less than one chunk, will incur a greater disk space percentage overhead since they must use at least a single chunk.

Another structure required for transactional semantics on LOBs is the LOB Index. Each LOB index entry can point to 8 chunks of a specific LOB object (`NumLobPerIndexEntry = 8`). In our continuing example, where a 500K file takes up 16 chunks, two index entries would be required for that object. Each entry takes 46 bytes (`LobIndexEntryOverhead`) and is then stored in an Oracle B*tree index, which in turn has its own overhead depending upon how fragmented that index becomes.

The last factor affecting LOB space utilization is the `PCTVERSION` parameter used when creating the LOB column. For information about how `PCTVERSION` works, please consult the *Oracle Database SQL Reference*.

Oracle Content DB uses the default `PCTVERSION` of 20 percent for the LOB columns it creates. This reduces the possibility of "ORA-22924 snapshot too old" errors occurring in read consistent views. So by default, a minimum of a 20 percent increase in chunking space must be added in to the expected disk usage to allow for persistent `PCTVERSION` chunks.

For large systems where disk space is an issue, Oracle recommends reducing `PCTVERSION` to 1, in order to reduce disk storage requirements. This may be done at any time in a running system using the following SQL commands:

```
alter table odmm_contentstore modify lob (globalindexedblob) (pctversion 1);
alter table odmm_contentstore modify lob (emailindexedblob) (pctversion 1);
alter table odmm_contentstore modify lob (emailindexedblob_t) (pctversion 1);
alter table odmm_contentstore modify lob (intermediablob) (pctversion 1);
alter table odmm_contentstore modify lob (intermediablob_t) (pctversion 1);
alter table odmm_nonindexedstore modify lob (nonindexedblob2) (pctversion 1);
```

The steps for calculating LOB tablespace usage are as follows:

1. Calculate the number of chunks a file will use by figuring the number of blocks per chunk, then subtracting the BlockOverhead (60 bytes) from the chunk size to get the available space per chunk.
2. Divide the file size by the available space per chunk to get the number of chunks, per the following formula:

   ```
   chunks = roundup(FileSize / ChunkSize=((ChunkSize/BlockSize) * BlockOverhead)))
   ```

   For example, if *`FileSize`* = 100,000, *`ChunkSize`* = 32768, *`Blocksize`* = 8192, and *`BlockOverhead`* = 60, then:

   ```
   roundup(100000 / (32768 - ((32768 / 8192) * 60))) = 4 chunks
   ```

3. Calculate the amount of disk space for a file by multiplying the number of chunks times the chunk size, multiplying that result by the `PCTVERSION` factor, and then adding the space for `NumLobPerIndexEntry` (8) and `LobIndexEntryOverhead` (46 bytes).

   ```
   FileDiskSpaceInBytes = roundup(chunks * ChunkSize * PCTVERSIONFactor) +
   roundup(chunks / NumLobPerIndexEntry * LobIndexEntryOverhead)
   ```

   Hence, if *`chunks`* = 4, *`ChunkSize`* = 32768, *`PCTVERSIONFactor`* = 1.1, *`NumLobPerIndexEntry`* = 8, and *`LobIndexEntryOverhead`* = 46:

   ```
   roundup(4 * 32768 * 1.1) + (roundup(4 / 8) * 46)= 144226 FileDiskSpaceInBytes
   ```

4. Calculate the total disk space used for file storage by summing up the application of the preceding formulas for each file to be stored in the LOB, per the formula:

   ```
   TableSpaceUsage = sum(FileDiskSpaceInBytes)
   ```

   for all files stored

Oracle Content DB creates multiple LOB columns. The space calculation must be made for each tablespace based upon the amount of content that will qualify for storage in that tablespace.

Oracle Content DB Metadata and Infrastructure

The Oracle Content DB server keeps persistent information about the file system and the contents of that file system in database tables. These tables and their associated structures are stored in the `CONTENT_IFS_MAIN` tablespace. This tablespace contains approximately 300 tables and 500 indexes. These structures are required to support both the file system and the various protocols and user interfaces that make use of that file system.

The administration and planning tasks of this space should be very similar to operations on a normal Oracle database installation. The administrator of the system should plan for approximately 6K of overhead per file to be used from this tablespace, or about 2% of the overall content. If there is a significant amount of custom metadata, such as categories, this overhead will be larger.

The initial disk space allocated for this tablespace is approximately 50MB for a default install. Of this 50MB, 16MB is actually used at the completion of installation. This includes instantiations for all required tables and indexes and the metadata required for the approximately 700 files that are loaded into Oracle Content DB as part of the install. Different tables and indexes within this tablespace will grow at different rates depending on which features of Oracle Content DB are used in a particular installation.

Oracle Text

When Oracle Content DB works in conjunction with Oracle Text, it allows users to access powerful search capabilities on the files stored within Oracle Content DB. Disk space for these capabilities is divided among three distinct tablespaces for optimal performance.

The `CONTENT_IFS_CTX_I` tablespace contains tables which hold the text tokens (separate words) that exist within the various indexed files. The storage for these text tokens is roughly proportional to the ASCII content of the file.

The ASCII content percentage varies depending on the format of the original file. Text files only have white space as their non-ASCII content and therefore incur a greater per file percentage overhead. File types such as Microsoft Word or PowerPoint contain large amounts of data required for formatting that does not qualify as text tokens. The per file percentage on these types of files is therefore lower. On a system with diverse content types the expected overhead is approximately 8% of the sum of the original sizes of the indexed files.

Table 2–8 offers general guidelines for the amount of ASCII text in a file for several popular formats:

Table 2–8 Average ASCII Content Per File Type

Format	Plain ASCII Content as Percentage of File Size	Typical Percentage of all File Content[1]
Microsoft Excel[2]	250%	4%
ASCII	100%	2%
HTML	90%	10%
Rich Text Format	80%	2
Microsoft Word	70%	13%
Acrobat PDF	10%	18%
Microsoft PowerPoint	1%	3%
Images (JPEG, BMP), Compressed files (Zip, TAR), Binary files, and so on.	0%	50%
Total		**100%**

[1] From statistics of Oracle Corporation's internal usage of Oracle Content DB.

[2] By default, Oracle Text indexes each number in an Excel file as a separate word. Excel stores a number more efficiently than its ASCII equivalent, which is why the ASCII content as a percentage of the file size is greater than 100%.

The `CONTENT_IFS_CTX_K` tablespace contains the tables and indexes required to translate from the Oracle Content DB locator of a file (the Oracle Content DB DocID) to the Oracle Text locator of that same file (the Oracle Text DocID). The expected space utilization for this tablespace is approximately 70 bytes per indexed file.

The `CONTENT_IFS_CTX_X` tablespace contains the B*tree database index that is used against the text token information stored in the `CONTENT_IFS_CTX_I` tablespace. This will grow as a function of the ASCII content just as the `CONTENT_IFS_CTX_I` tablespace does. On a system with diverse content types the expected overhead is approximately 4% of the sum of the ASCII content of the files, or approximately 1% of the sum of the total sizes of the indexed files.

Disk Space Requirements: Sample Deployment

This section details various requirements for disk space, and offers guidance as to how necessary disk space will expand with the addition of files to the server.

Based on experience running Oracle Content DB for Oracle Corporation's internal usage, the disk overhead of Oracle Content DB for a large system (hundreds of gigabytes of file content) is approximately as detailed in Table 2–9.

Table 2–9 Disk Space Requirements Summary

Tablespace Overhead Type	Overhead Versus Total Raw File Content[1]	Primarily Determined By
File Storage	12%	Size of files relative to chunk size (32KB by default)
Oracle Text	5%	Amount of ASCII content in all files
Metadata	2%	Number of folders, files, and so on.
General Oracle Storage	1%	Fixed, not configurable, database settings for `TEMP`, `UNDO`, and other tablespaces
Total	**20%**	Not applicable

[1] This does not include: mirroring for backup and reliability; Redo log size, which should be determined by how many files are inserted and their size; unused portion of the last extent in each database file (which will occur with pre-created database files or which may be large if the next extent setting is large).

See *Oracle Database Concepts* for explanations of the terms Large Object, tablespace, chunk size, and extents.

Given that a large percentage of the overhead is in LOB overhead, note that the overhead for your Oracle Content DB instance may vary depending on the average and median sizes of files.

3

Oracle Content DB Security

Oracle Content DB provides the basic infrastructure required by any shared, network-accessible system, including authentication and authorization. This chapter describes the architecture and configuration of security in Oracle Content DB.

This chapter provides information about the following topics:

- User Authentication
- Security Considerations for Protocol Servers
- Malicious Uploads
- Client Session Timeout Period
- SSL Configuration for Oracle Content DB
- Changing the Oracle Content DB Schema Password
- Oracle Records DB

Note: Do not make any configuration changes to your Oracle Content DB deployment beyond those described in the documentation or required by the support team. Making undocumented changes to your system could have serious security implications.

User Authentication

Authentication is a process in which a user provides some proof of identity (called a *credential*, which is often constructed from a user's password by means of a hashing or encryption algorithm) before that user can attempt to access objects in the system. Oracle Content DB uses Oracle Internet Directory, Oracle's LDAP-compliant directory service, for authentication.

Users provide their user name and password to the client software. These are passed to the Oracle Content DB protocol servers, which, in turn, pass them to Oracle Content DB for authentication. Then, Oracle Content DB passes the user name and password to Oracle Internet Directory. Oracle Internet Directory determines whether the user name and password are valid for the user.

Note: The information provided in this section is a high-level, simplified description and may not include all the interaction that occurs. See *Oracle Internet Directory Administrator's Guide* for more information about how Oracle Internet Directory handles user authentication.

Security Considerations for Protocol Servers

This section describes the security considerations for protocol servers and contains the following topics:

- FTP and FTPS
- HTTP and WebDAV
- Network Channel Encryption

Note: The defined behavior of some industry-standard protocols is not inherently secure. Oracle has no control over the defined behavior of these protocols, and these security issues do not represent defects in Oracle software.

FTP and FTPS

The File Transfer Protocol (**FTP**) sends unencrypted user passwords across the network, which means that if one of these passwords is intercepted, then it could provide access to all systems controlled by Oracle Internet Directory for that user. To provide more security, users must create an FTP password (separate from their single sign-on password) to authenticate against FTP. Users should not use the same value for their FTP password and their single sign-on password.

The FTP password is stored in Oracle Internet Directory and is different from and in addition to the regular Oracle Internet Directory password. Each user can have only one FTP password in one Oracle Content DB domain. FTP requires users to log in with an FTP password rather than an Oracle Internet Directory password.

Users can set their FTP password on the User Preferences page in Oracle Content DB. Users can also use the Oracle Internet Directory Self-Service Console to set their FTP password, by setting the content password entry that appears in the Application Passwords section of the Change Password page.

As an alternative, users can use **FTPS**. FTPS is FTP with the added option of Secure Socket Layer (SSL) security. FTPS does not require an FTP password.

By default, the FTP and FTPS servers are disabled in Oracle Content DB. See "Using FTP with Oracle Content DB" on page 4-2 for full information about FTP and FTPS.

HTTP and WebDAV

The HTTP and WebDAV protocols allow *digest* (hashed challenge/response) and persistent cookie (if the domain and then the user enables the feature) authentication. Whether HTTP and WebDAV use SSL depends on the configuration of Oracle HTTP Server and on whether Oracle Content DB has been configured for SSL.

Oracle Drive is a desktop client that uses the WebDAV protocol to access Oracle Content DB. After it is installed, Oracle Drive appears as a mapped drive in Windows

Explorer. Oracle Drive also provides file synchronization capabilities between your local computer and Oracle Content DB.

Network Channel Encryption

The FTP, HTTP, and WebDAV protocols do not encrypt the network channel by default. This means that files transferred using these protocols are susceptible to interception. If you are unwilling to accept this behavior, then you should disable these protocols or configure them to use SSL.

See "SSL Configuration for Oracle Content DB" on page 3-4 for more information.

Malicious Uploads

Because user quota is managed asynchronously through the Quota Agent, it is possible for a malicious user to upload a very large file for filling up disk space. To prevent such attacks, you can limit the size of any single file uploaded to Oracle Content DB by setting the `IFS.DOMAIN.MEDIA.CONTENTTRANSFER.ContentLimit` domain property. If you try to upload a file beyond the specified limit, then the upload fails. This limit does not apply to administrators.

When this property is set to `0`, the default value, the content limit is disabled. You will be able to upload any file whose size is within the last calculated available quota, as of the beginning of the upload.

If you choose to set this limit, make sure the value you specify is not too low so that regular users do not encounter upload failures when uploading large files.

See "Changing Domain Properties" on page 8-1 for more information about setting the `IFS.DOMAIN.MEDIA.CONTENTTRANSFER.ContentLimit` property.

Client Session Timeout Period

The *client session timeout period* is the number of minutes of idle time after which a Web user interface session expires. By default, the client session timeout for Oracle Content DB is set to 30 minutes. To change this value, perform the following steps:

1. Access the Application Server Control and go to the Application Server Home page.
2. Select **OC4J_Content** and click **Stop**.
3. Click **OC4J_Content** to go to the OC4J_Content Home page.
4. Click **Applications**, then click **content** in the Deployed Applications table.
5. On the Applications: content page, click **content** in the Web Modules table.
6. On the Web Module: content page, in the Administration section, click **General** under the Properties heading.
7. In the Session Configuration section, change the value for **Session Timeout (minutes)**.
8. Click **Apply**, then click **OK** on the Confirmation page.
9. Return to the Application Server Home page, select **OC4J_Content**, and click **Start**.

If you have enabled Oracle Records DB, then you can also set the client session timeout period for Oracle Records DB. Repeat these steps for OC4J_RM to change the client session timeout period for Oracle Records DB.

SSL Configuration for Oracle Content DB

You must configure Oracle HTTP Server to use SSL before configuring Oracle Content DB for SSL. See *Oracle Application Server Administrator's Guide* for more information.

After configuring Oracle HTTP Server for SSL, follow these steps to configure Oracle Content DB for SSL:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Domain Properties**.
3. Click **IFS.DOMAIN.APPLICATION.ApplicationPort**.
4. Update the value to the Oracle HTTP Server SSL port and click **OK**.
5. Click **IFS.DOMAIN.APPLICATION.ApplicationUseHttps**.
6. Set the value to **true** and click **OK**.
7. Return to the Content DB Home page and click **Restart Domain**.

Connecting to Oracle Internet Directory Using SSL

Before you can configure Oracle Content DB to use SSL to connect to Oracle Internet Directory, Oracle Internet Directory must be configured for SSL. See *Oracle Internet Directory Administrator's Guide* for more information.

To configure Oracle Content DB to use SSL to connect to Oracle Internet Directory:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Service Configurations**.
3. Click the name of the service configuration you are using (for example, **LargeServiceConfiguration**).
4. In the Properties section, click **IFS.SERVICE.CREDENTIALMANAGER.Oid.OidSsl**. You may need to move to the next page to find this property, or you can use the **Search** field.
5. Set the **Value** to true and click **OK**.
6. Click **IFS.SERVICE.CREDENTIALMANAGER.Oid.OidUrl**.
7. Change the port number listed in the URL to be the SSL-enabled Oracle Internet Directory port, typically 636 or 4031, and click **OK**.
8. Click **OK** on the Edit Service Configuration page.
9. Return to the Content DB Home page and click **Restart Domain**.

Changing the Oracle Content DB Schema Password

The Oracle Content DB schema password is stored in the following locations:

- Oracle Database
- Oracle Internet Directory
- Any Oracle Content DB middle tier where you are running repository metrics

You can use the Application Server Control to change the Oracle Content DB schema password. The password will be changed in Oracle Internet Directory, as well as:

- On the current middle tier, if you are running repository metrics on this middle tier

- In the Oracle Database, if you select **Change in Database**

You should only change the schema password from the middle tier on which repository metrics are being collected. If you are collecting repository metrics on more than one middle tier, you must change the schema password on all middle tiers where repository metrics are collected. If you are not collecting any repository metrics, it does not matter which middle tier you choose to use. See "Monitoring Domain Performance" on page 9-1 for more information about repository metrics.

To change the Oracle Content DB schema password:

1. Connect to the Application Server Control on the middle tier where you want to change the schema password.
2. Go to the Content DB Home page.
3. Click **Stop Domain**.
4. In the Administration section, click **Change Schema Password**. You will not be able to access the Change Schema Password page unless all Oracle Content DB processes have been stopped.
5. In the **Password** field, enter the new password. Then, in the **Confirm Password** field, enter the password again.
6. If the schema password has not yet been changed in the database, you can choose to change the database schema password at this time. To do this, select **Change in Database** and provide the database SYS password.
7. Click **OK**.
8. Return to the Content DB Home page and click **Start Domain**.

Oracle Records DB

Oracle Records DB is a records management application that ships with Oracle Content DB.

When you install Oracle Content DB, Oracle Records DB is installed automatically, but the application is disabled by default. You can use the Application Server Control to enable Oracle Records DB. You can also configure metrics related to Oracle Records DB. See "Setting Up Oracle Records DB" on page 5-1 for more information.

Using a Retention Hardware Solution

Oracle Content DB provides retention hardware capabilities through partnerships with Network Appliance and EMC. You can use the Application Server Control to integrate Oracle Content DB with Network Appliance SnapLock or EMC Centera.

To integrate Oracle Content DB with a records management retention device, you must first install the hardware (either EMC Centera or Network Appliance SnapLock). Then, you must specify credential information for the hardware and set retention-related domain properties using the Application Server Control. See "Integrating with Solutions for Records Management Retention" on page 5-9 for more information.

Once you have created a file plan and defined retention policies in Oracle Records DB, Oracle Content DB will designate appropriate content as records to be stored in a records management retention device.

4

Oracle Content DB Protocol Support

This chapter discusses the protocol servers supported by Oracle Content DB, and the client access paths and software for the supported protocols.

This chapter provides information about the following topics:

- About the Oracle Content DB Protocol Servers
- Using FTP with Oracle Content DB
- Using WebDAV with Oracle Content DB
- Authenticating Against WebDAV and FTP
- Using Oracle Drive with Oracle Content DB

About the Oracle Content DB Protocol Servers

Users can connect to Oracle Content DB using protocols appropriate to their platform. For example, Windows users can use the Oracle Drive client or connect using Web Folders, Macintosh users can connect through WebDAV, and UNIX users can connect using FTP. Users on all platforms can connect using HTTP for browser-based access.

Oracle Content DB supports the following protocols:

- **HTTP** is used for browser-based access. Use the following URL to access Oracle Content DB with HTTP:

  `http://server_name:port/content`

- **FTP** is used for file transfers across wide area networks such as the Internet.

  The FTP protocol sends unencrypted passwords over the network. For this reason, users must create an FTP password for greater security. See the "Oracle Content DB Security" chapter on page 3-1 for more information about FTP passwords.

  In addition to FTP, **FTPS** is supported. You can access Oracle Content DB using either implicit or explicit FTPS. Because FTPS does not send unencrypted passwords over the network, an FTP password is not necessary.

- **WebDAV**, Web-based Distributed Authoring and Versioning, is an HTTP-related protocol that is designed for wide area networks such as the Internet. Currently, the most widespread WebDAV client is the Web Folders extension to Windows Explorer, also known as Network Places in Windows 2000 and Windows XP. Oracle Content DB also provides WebDAV support for Macintosh users.

  The Oracle Drive client provides Windows users with SMB-like drive mapping capabilities, while using WebDAV as the actual file protocol.

Table 4–1 lists some of the client platforms, protocols, and access methods supported by Oracle Content DB. See Oracle*MetaLink* at `http://metalink.oracle.com` for complete client certification information.

Table 4–1 Client Platforms and Protocol Support

Client Platform	Protocols Supported	Access Using[1]
Windows	HTTP, WebDAV, FTP/FTPS	Browser, Oracle Drive, Windows Explorer, FTP/FTPS client
Macintosh (Mac OS 10.3)	HTTP, WebDAV, FTP/FTPS	Browser, WebDAV client, FTP client
UNIX	HTTP, FTP/FTPS	Browser, command line
Red Hat Linux Adv. Server 3.0 (Kernel 2.4.9-e.16)	HTTP, FTP/FTPS	Browser, command line

[1] For all protocols, if the server to which you are connecting uses DHCP, then you must use the current IP address of the host in the connection syntax instead of the host name.

Using FTP with Oracle Content DB

FTP can move large amounts of data faster than the other protocols. For bulk operations, such as migrating files from an existing system, FTP is the preferred protocol. FTP is disabled, by default, after Oracle Content DB is installed and configured.

Oracle Content DB also supports FTPS, which uses SSL to provide a confidential, integrity-protected channel. FTPS defines a mechanism to implement the FTP Security Extensions based on the TLS protocol. There is wide support for FTPS among FTP clients. Do not confuse FTPS with SFTP, a service of the Secure Shell that is not related to FTP. FTPS is also disabled, by default, after Oracle Content DB is installed and configured.

Note that if you define a policy on a folder or Library that requires users to enter data associated with uploaded content, users will not be able to place content in that folder or Library using FTP. This limitation is because the FTP protocol does not provide a facility to enter metadata.

This section contains the following topics:

- Accessing Oracle Content DB Using FTP or FTPS
- Enabling FTP
- Enabling Anonymous FTP Access
- Enabling FTPS

Accessing Oracle Content DB Using FTP or FTPS

After FTP or FTPS has been enabled, users can use FTP or FTPS with Oracle Content DB, as long as the following requirements are met:

- An FTP or FTPS client must be installed on the local computer of the user.
- The user must know which port number to use. The default port number for FTP and for explicit FTPS is 21; the default port number for implicit FTPS is 990.
- For FTP only, each user must use a separate FTP password for greater security. Users can set their FTP password on the User Preferences page in the Oracle Content DB Web client.

- Users who are not members of the default Site must specify their realm name when they access Oracle Content DB through FTP or FTPS, in the format `username@realmname`.

Oracle Content DB supports several FTP Quote commands that users can issue during an FTP or FTPS session. See Appendix F, "FTP Quote Command Reference" for more information.

Note that users with multibyte user names cannot sign on to Oracle Content DB using FTP. For this reason, you should not create Oracle Content DB user names that contain multibyte characters.

Enabling FTP

You can enable FTP for Oracle Content DB so that users can upload and download files using FTP. FTP is disabled, by default, after Oracle Content DB is installed and configured.

To enable the Oracle Content DB FTP server:

1. Access the Application Server Control and go to the Content DB Home page.
2. You may want to change the default port number for the FTP server. To do this:
   a. In the Administration section, click **Server Configurations**.
   b. Click **FtpServerConfiguration**.
   c. In the Properties section, click **IFS.SERVER.PROTOCOL.FTP.Port**.
   d. In the **Value** field, enter the desired port number and click **OK**.
   e. On the Edit Server Configuration page, click **OK**.
3. Return to the Content DB Home page, and in the Administration section, click **Node Configurations**.
4. Click the name of the node configuration that corresponds to the node where you want to run the FTP server. You can only run the FTP server on regular nodes; you cannot run FTP on HTTP nodes.
5. Scroll down to the Servers table and click **FtpServer**.
6. Select **Active** and **Initially Started**.
7. On the Edit Server page, click **OK**.
8. On the Edit Node Configuration page, click **OK**.
9. Return to the Content DB Home page and restart the node.

Repeat this procedure for any additional regular nodes on which you want to run FTP.

Enabling Anonymous FTP Access

For security reasons, anonymous FTP access is disabled by default. If you want to enable anonymous access, you must first modify the FTP server configuration to allow anonymous access, then allow public access to particular folders in Oracle Content DB.

After public access has been enabled for a particular folder, users can connect directly to that folder using anonymous FTP. In most cases, anonymous users should use FTP links to connect. For example, if an administrator only enables public access to the folder `/us/TestFiles/PublicViewing`, users would need to configure an FTP client to connect directly to that folder. Anonymous users would not be able to connect to the root folder and navigate to the `PublicViewing` folder, because the `us` and `TestFiles` folders do not have public access enabled.

Modifying the FTP Server Configuration

To modify the FTP server configuration to allow anonymous access:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Server Configurations**.
3. Click **FtpServerConfiguration**.
4. In the Properties section, select **IFS.SERVER.PROTOCOL.FTP.AnonymousAllowed** and click **Edit**, or just click the property name.
5. Set the **Value** to true and click **OK**.
6. On the Edit Server Configuration page, click **OK**.
7. Return to the Content DB Home page and restart the node.

Enabling the Ability to Grant Public Access

Before you can allow public access to a particular folder, you must ensure that the ability to grant public access has been enabled at the Site level.

To ensure that the ability to grant public access is enabled for the Site:

1. Connect to Oracle Content DB as a user with the Content Administrator and User Administrator roles, such as `orcladmin`.
2. Change to Administration Mode.
3. Access the Sharing Properties for the root Site folder.
4. Ensure that the option **Allow public access to be granted** has been enabled.

Allowing Public Access to Oracle Content DB Folders

To grant public access to a particular folder:

1. Connect to Oracle Content DB as a user with the Content Administrator and User Administrator roles, such as `orcladmin`.
2. Change to Administration Mode.
3. Access the Sharing Properties for the folder to which you want to grant public access.
4. Add the special group **Public** to this folder. If you cannot add this group, make sure that you enabled the ability to grant public access at the Site level, as described in the previous procedure.

Enabling FTPS

You can enable FTPS for Oracle Content DB so that users can upload and download files using FTPS. The FTPS protocol is disabled, by default, after Oracle Content DB is installed and configured. Users sign on to Oracle Content DB over FTPS using their regular single sign-on password.

There are two types of FTPS supported by Oracle Content DB: implicit FTPS and explicit FTPS. Implicit FTPS secures the channel on connection, while explicit FTPS (Auth TLS) secures the connection when the client issues an AUTH command. An explicit FTPS connection starts out as a regular FTP connection; the connection becomes secure only after the client issues an AUTH command. You can choose to enable the implicit FTPS server, the explicit FTPS server, or both.

To set up FTPS, you first need to use Oracle Wallet Manager to create a new wallet and obtain a security certificate. You must configure the wallet for automatic login. For more information, see *Oracle Database Advanced Security Administrator's Guide*.

After you have obtained a security certificate, you can use the Application Server Control to enable the Oracle Content DB FTPS servers.

Enabling the Explicit FTPS Server

To enable explicit FTPS:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Server Configurations**.
3. Click **FtpsServerExplicitConfiguration**.
4. Select **IFS.SERVER.PROTOCOL.FTP.Port** and click **Edit**, or just click the property name.
5. In the **Value** field, enter the appropriate Explicit FTPS port number (for example, 21) and click **OK**.
6. Select **IFS.SERVER.PROTOCOL.FTPS.WALLET.Location** and click **Edit**, or just click the property name.
7. Update the value with the location of the wallet file (for example, `/CSHome/WALLET/cwallet.sso`) and click **OK**.
8. On the Edit Server Configuration page, click **OK**.
9. Return to the Content DB Home page and click **Node Configurations** in the Administration section.
10. Click the name of the regular node configuration that corresponds to the node where you want to run the Explicit FTPS server.
11. In the Servers section, select **FtpsServerExplicit** and click **Edit**, or just click the server name.
12. Select **Active** and **Initially Started**, then click **OK**.
13. On the Edit Node Configuration page, click **OK**.
14. Return to the Content DB Home page and restart the node.

Enabling the Implicit FTPS Server

To enable implicit FTPS:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Server Configurations**.
3. Click **FtpsServerImplicitConfiguration**.
4. Select **IFS.SERVER.PROTOCOL.FTP.Port** and click **Edit**, or just click the property name.
5. Update the **Value** with the appropriate Implicit FTPS port number (for example, 990) and click **OK**.

6. Select **IFS.SERVER.PROTOCOL.FTPS.WALLET.Location** and click **Edit**, or just click the property name.
7. Update the value with the location of the wallet file (for example, `/CDBHome/WALLET/cwallet.sso`) and click **OK**.
8. On the Edit Server Configuration page, click **OK**.
9. Return to the Content DB Home page and, in the Administration section, click **Node Configurations**.
10. Click the name of the regular node configuration that corresponds to the node where you want to run the Implicit FTPS server.
11. Select **FtpsServerImplicit** and click **Edit**, or just click the server name.
12. Select **Active** and **Initially Started**, then click **OK**.
13. On the Edit Node Configuration page, click **OK**.
14. Return to the Content DB Home page and restart the node.

Using WebDAV with Oracle Content DB

The WebDAV protocol is enabled, by default, after Oracle Content DB is installed and configured.

Note that if you define a policy on a folder or Library that requires users to enter data associated with uploaded content, users will not be able to place content in that folder or Library using WebDAV. This limitation is because the WebDAV protocol does not provide a facility to enter metadata.

Accessing Oracle Content DB Using WebDAV

Use the following URL to access Oracle Content DB with WebDAV:

```
http://server_name:port/content/dav
```

The value for *`port`* varies depending on your platform, and depending on whether OracleAS Web Cache is running. If OracleAS Web Cache is running, the typical values are:

- 7777 for UNIX systems
- 80 for Windows systems (unless port 80 is in use when the middle tier is configured)

If OracleAS Web Cache is not running, the port number is typically 7778.

Users who are not members of the default Site must specify their realm name when they access Oracle Content DB through WebDAV, in the format `username@realmname`.

Note that users with multibyte user names cannot sign on to Oracle Content DB using WebDAV. For this reason, you should not create Oracle Content DB user names that contain multibyte characters.

Authenticating Against WebDAV and FTP

The user name that needs to be entered when authenticating against WebDAV and FTP can vary. The user name format depends on whether the user is a member of the default realm, and on the nickname attribute set for the realm in Oracle Internet Directory (`uid` or `mail`).

The default nickname attribute is `uid`. You can use Oracle Directory Manager to view or change the nickname attribute for the realm; see *Oracle Internet Directory Administrator's Guide* for more information about using Oracle Directory Manager.

Table 4–2 summarizes the user name format that users need to enter for WebDAV and FTP, according to these two factors.

Table 4–2 User Name Format for Authenticating Against WebDAV and FTP

Realm Type	Nickname Attribute	Example User Names in Oracle Internet Directory	Example User Names to Enter When Authenticating Against WebDAV and FTP
Default realm Example: oracle	uid	user_name jsmith	user_name jsmith
Non-default realm Example: mycompany	uid	user_name jsmith	user_name@mycompany jsmith@mycompany
Default realm Example: oracle	mail	user.name@mydomain.com jsmith@anotherdomain.com	user.name jsmith
Non-default realm Example: mycompany	mail	user.name@mydomain.com jsmith@anotherdomain.com	user.name@mycompany jsmith@mycompany

Using Oracle Drive with Oracle Content DB

Oracle Drive is a native Windows application that lets users use Windows Explorer, Microsoft Office, and other Windows applications to access content in Oracle Content DB and other Oracle WebDAV servers such as OracleAS Portal. Oracle Drive displays files and folders in Oracle Content DB as a mapped drive in Windows Explorer. Oracle Drive also provides an effective offline solution that lets users edit files on their computers when offline, and then synchronize with the server when they reconnect.

Oracle Drive is available on the Oracle Drive client CD that comes with the Oracle Content DB software.

Oracle Drive runs on Microsoft Windows 2000 and Windows XP. For the most up-to-date certification information, see Oracle*MetaLink* at `http://metalink.oracle.com`.

Oracle Drive requires Microsoft .NET Framework 1.1. The Oracle Drive installation installs the Microsoft .NET Framework 1.1 on the client computer.

You can set up an administrator-configured installation of Oracle Drive so that Oracle Drive is automatically deployed on user workstations, or you can copy the Oracle Drive executable to an accessible location so that users can install Oracle Drive themselves. You can also include service details with the Oracle Drive executable so that users don't have to configure their Oracle Drive service. The following sections provide more information about these topics:

- Setting Up an Administrator-Configured Installation of Oracle Drive
- Packaging Service Information with the Oracle Drive Executable
- Installing Oracle Drive from the Client CD

Setting Up an Administrator-Configured Installation of Oracle Drive

Setting up an automatic installation of Oracle Drive for your users is strongly encouraged. Oracle Drive is the client of choice for uploading and downloading many files at once, and also provides synchronization capabilities. Setting up an administrator-configured install will encourage user adoption and reduce support calls.

Configuring Oracle Drive Service Details For Your Users

You can choose to specify Oracle Drive service details as part of your Oracle Drive deployment. Setting up an Oracle Drive service for your users is strongly recommended so that users do not have to configure Oracle Drive themselves. Note that individual users can still edit service details as necessary for their own computers.

To specify Oracle Drive service details, update the parameters in the `config.xml` file. Then, specify the location of the `config.xml` file in the `update.xml` file. Both of these files need to be copied to an HTTP server that is accessible to all your users, without requiring a login.

Finally, specify the location of the `update.xml` file in `odrive.ini`, then copy it to the same location as the `ODriveSetup.msi` file. See the "Preparing for Deployment Using Active Directory" on page 4-11 for more information about `ODriveSetup.msi`.

These steps are detailed in the following sections:

- Setting Up config.xml
- Setting Up update.xml
- Setting Up odrive.ini

Setting Up config.xml The `config.xml` file contains the details for the Oracle Drive service you want to deploy. Update `config.xml` by providing your own values for each parameter. Then, copy the file to an HTTP server that is accessible to all your users, without requiring a login. You can find `config.xml` in the `\Extra` folder on the Oracle Drive client CD.

You can configure multiple services for your users by providing additional `<item>` entries, with parameters, in `config.xml`. Refer to Table 4–3 for information about the parameters in `config.xml`.

Example 4–1 shows the format of the `config.xml` file, with sample values for two services.

Example 4–1 config.xml

```
<wfc-config>

<item>
  <type>service</type>
  <name>Oracle Content DB</name>
  <hostname>myhost1.company.com</hostname>
  <port>7777</port>
  <secure>1</secure>
  <server-directory>/users/mydir</server-directory>
  <drive-letter>k</drive-letter>
  <sharing-level>3</sharing-level>
  <map-home>1<map-home>
  <auto-reconnect>2</auto-reconnect>
  <basic-authentication>0</basic-authentication>
</item>
```

```
<item>
  <type>service</type>
  <name>Oracle Portal</name>
  <hostname>myhost2.company.com</hostname>
  <port>7778</port>
  <secure>1</secure>
  <server-directory>/my_location</server-directory>
  <drive-letter>z</drive-letter>
  <sharing-level>3</sharing-level>
  <map-home>1<map-home>
  <auto-reconnect>2</auto-reconnect>
  <basic-authentication>0</basic-authentication>
</item>

</wfc-config>
```

Table 4–3 Parameter Values for config.xml

Parameter Name	**Description**
<type>	The value for this parameter must always be "service." Do not change this value.
<name>	The name of the service (for example, Oracle Content DB) as it will appear in Oracle Drive.
<hostname>	The host name of the Oracle Content DB server (for example, `myhost.mycompany.com`).
<port>	The port number of the Oracle Content DB server (for example, 7778). If you do not specify this value, the port number defaults to either `80` or `443`, depending on the value you specify for `<secure>`.
<secure>	Whether HTTP or HTTPS will be used to connect to Oracle Content DB. The possible values are: - `0` (use HTTP) - `1` (use HTTPS)
<server-directory>	The Oracle Content DB folder location to mount, or in other words, the folder location that will appear as the top-level folder when users connect to Oracle Content DB using Oracle Drive (for example, `/content/dav/my_site/Libraries/mydir`). You must include `/content/dav` at the beginning of the specified path.
<drive-letter>	The Windows drive letter to use for this service. The value can be any drive letter from D-Z. If you do not specify a value, or if the letter you specify is not available, the first drive letter available will be used.

Table 4–3 (Cont.) Parameter Values for config.xml

Parameter Name	Description
<sharing-level>	The default value for the refresh interval to use for this service. The longer the refresh interval, the better the performance. However, when the refresh interval is longer, files and directories are refreshed less frequently, so users may notice a lag in seeing file and directory changes made by other users. In addition, the longer the refresh interval, the fewer server resources are needed (such as CPU or disk I/O). The possible values are: ■ `0` (1 hour) ■ `1` (15 minutes) ■ `2` (3 minutes) ■ `3` (15 seconds)
<map-home>	Whether to map to the Personal Library of the user by default (if the Personal Library exists). The possible values are: ■ `1` (map to the Personal Library of the user) ■ `2` (do not map to the Personal Library of the user) The Personal Library can only be mounted if the value for `<server-directory>` begins with `/content/dav`.
<basic-authentication>	Whether users can use basic authentication to connect to WebDAV servers that require cleartext passwords. The possible values are: ■ `0` (do not use basic authentication) ■ `1` (use basic authentication) Because Oracle Content DB does not require cleartext passwords, enter `0` for this parameter.
<auto-reconnect>	Whether or not to automatically connect to the service when Oracle Drive starts. The possible values are: ■ `1` (automatically connect to the service) ■ `2` (do not automatically connect to the service)

Setting Up update.xml The `update.xml` file holds the value for the location of the `config.xml` file. You can find `update.xml` in the `Extra` folder on the Oracle Drive client CD.

Edit the `update.xml` file by providing your own values for each parameter:

- `<date>`: Provide a string value (such as a date, in any format, or other representation) that corresponds to the configuration file version you are using. If Oracle Drive detects that the string value has changed since the last time it started, Oracle Drive will process the new `config.xml` file.
- `<location>`: Provide the URL to `config.xml`.

Then, copy the file to an HTTP server that is accessible to all your users, without requiring a login.

Example 4–2 shows the format of the `update.xml` file, with sample values.

Example 4–2 update.xml

```
<?xml version="1.0" ?>
<config-update>
```

```
  <date>2006.07.31 13:41:PST</date>
  <location>http://myserver.mycompany.com/config.xml</location>
</config-update>
```

Setting Up odrive.ini The `odrive.ini` file holds the value for the location of the `update.xml` file. You can find `odrive.ini` in the `Extra` folder on the Oracle Drive client CD.

Update `odrive.ini` by providing the URL for your `update.xml` file, then copy `odrive.ini` to the same directory where the `ODriveSetup.msi` file is located. See the "Preparing for Deployment Using Active Directory" on page 4-11 for more information about `ODriveSetup.msi`.

Example 4–3 shows the format of the `odrive.ini` file, with sample values.

Example 4–3 odrive.ini

```
[General]
AutoupdateURL=http://myserver.mycompany.com/odrive/update.xml
```

Preparing for Deployment Using Active Directory

You must use a Windows Domain Controller computer to deploy Oracle Drive using Active Directory. If you need to promote a Windows 2000 or 2003 server to be a Domain Controller, you can use the Microsoft utility `DCPromo.exe`.

You must also install Active Directory on the Domain Controller computer, if it is not installed already.

Finally, you must extract the `ODriveSetup.msi` file, along with other files required for installation, from the Oracle Drive installation executable. To do this:

1. Open a command prompt and navigate to the directory where the Oracle Drive executable is located.
2. Exit Oracle Drive, if it is running. To do this, right-click on the Oracle Drive icon in the system tray and choose **Exit**.
3. Run the Oracle Drive executable in administrative mode, as follows:

   ```
   executable_name /a
   ```

   For example:

   ```
   ODriveSetup10.2.0.0.0.exe /a
   ```

4. Follow the wizard instructions. On the Network Location screen, specify the location on your local (not network) drive where you want to put the MSI and other files.
5. Click **Finish** to exit the wizard.
6. Copy the files to a public share accessible to all the users of that domain. If you are specifying Oracle Drive service details for your users, make sure to copy `odrive.ini` to the same location.

Deploying Oracle Drive Using Active Directory

You can use Active Directory to automatically deploy Oracle Drive (using MSI) on user workstations. With this technique, you can deploy Oracle Drive on all computers for your users from a single server.

Microsoft Windows 2000 or later operating systems include tools that allow administrators to install and maintain software applications based on Group Policy. An administrator can assign Oracle Drive to a particular computer by creating a computer-level software distribution Group Policy. Assigning Oracle Drive to user computers is the simplest way to use Group Policy to manage a package. With this method, Oracle Drive is automatically installed on the computer the first time a designated computer is started and the software installation portion of the Group Policy is applied.

This feature allows administrators to set up the environment required for the whole group, including specifying Oracle Drive service details.

To set up an automatic installation of Oracle Drive using Active Directory and MSI:

1. From the Windows **Start** menu, choose **Active Directory for Users and Computers**. The Active Directory application appears.
2. In the tree view, under the domain name, create a new organization unit (for example, OdriveOU).
3. By default, all the computers in the domain appear in the Computers organization unit. Move the computers on which you want to deploy Oracle Drive to the new organization unit you created in Step 2.

   Oracle recommends you deploy Oracle Drive to a small subset of computers first, for testing purposes, before deploying to your entire organization.
4. Right-click the organization unit you created and select **Properties**.
5. Click the **Group Policy** tab and create a new group policy object link.
6. Double-click the group policy object link you created in Step 5. The Group Policy Object Editor appears.
7. In the tree view, go to **Computer Configuration** > **Software Settings** > **Software Installation**. Ensure that **Software Installation** is selected, then right-click in the right pane and choose **New** > **Package**.
8. Specify the extracted MSI file for the new package, then, in the Deploy Software dialog box, select **Advanced** for the deployment method.
9. After you have created the new package, right-click the package and select **Properties**. Click the **Deployment** tab and ensure that the **Deployment type** is set to **Assigned**, then click **OK**.

Any errors that occur during the deployment of Oracle Drive will appear in the Event Log for the Windows Domain Controller computer. The Event Log can be viewed locally, or remotely.

Most files installed with Oracle Drive are put in the Oracle Drive installation directory. In addition, Oracle Drive installs additional files in the `System32` directory for use by Windows. Table 4–4 lists these additional files.

Table 4–4 Files Installed by Oracle Drive Into the System32 Directory

File Name	File Location
`tdfsd.sys`	`Windows_folder\System32\Drivers`
`TDShell.dll`	`Windows_folder\System32`
`TDHook.dll`	`Windows_folder\System32`
`XDNP.dll`	`Windows_folder\System32`
`ODriveHelper.dll`	`Windows_folder\System32`

Redeploying Oracle Drive

You can upgrade the version of Oracle Drive on user workstations by redeploying Oracle Drive using Active Directory.

To redeploy Oracle Drive:

1. On the Windows Domain Controller computer, from the **Start** menu, choose **Active Directory for Users and Computers**. The Active Directory application appears.
2. In the tree view, right-click the organization unit you created for the Oracle Drive deployment and select **Properties**.
3. Click the **Group Policy** tab, then double-click the group policy object link. The Group Policy Object Editor appears.
4. In the tree view, go to **Computer Configuration** > **Software Settings** > **Software Installation**. Right-click the package in the right pane and choose **All Tasks > Redeploy application**.

Removing Oracle Drive from User Workstations

You can undeploy Oracle Drive from user workstations using Active Directory.

To undeploy Oracle Drive:

1. On the Windows Domain Controller computer, from the **Start** menu, choose **Active Directory for Users and Computers**. The Active Directory application appears.
2. In the tree view, right-click the organization unit you created for the Oracle Drive deployment and select **Properties**.
3. Click the **Group Policy** tab, then double-click the group policy object link. The Group Policy Object Editor appears.
4. In the tree view, go to **Computer Configuration** > **Software Settings** > **Software Installation**. Right-click the package in the right pane and choose **All Tasks > Remove**.

Packaging Service Information with the Oracle Drive Executable

As an alternative to automatically installing Oracle Drive on user workstations, you can provide service information as part of the Oracle Drive executable. Using this method, users install Oracle Drive themselves, but do not have to configure service details after installation completes.

To include service information with the Oracle Drive executable:

1. Copy the contents of the Oracle Drive client CD to a location on your local hard drive (for example, `C:\odrive`).
2. In the `Extra` folder, open the file `config.xml` in a text editor. Provide service details, then copy the file to an accessible location. See "Setting Up config.xml" on page 4-8 for more information.
3. In the `Extra` folder, open the file `update.xml` in a text editor. Provide the location of `config.xml`, then copy the file to an accessible location. See "Setting Up update.xml" on page 4-10 for more information.
4. In the `Extra` folder, open the file `odrive.ini` in a text editor and provide the location of `update.xml`. See "Setting Up odrive.ini" on page 4-11 for more information.

5. In the `Extra` folder, open the file `OracleDrive10.2.SED` in a text editor. Edit the `TargetName`, `SourceFiles0`, and `SourceFiles1` properties, as necessary:

   - For `TargetName`, provide the location where you want to put the Oracle Drive executable.
   - For `SourceFiles0`, provide the location on your hard drive where you copied the `Binaries` folder.
   - For `SourceFiles1`, provide the location on your hard drive where you copied the `Extra` folder.

   If you copied the Oracle Drive files to `C:\odrive`, you can keep the defaults and skip this step.

   The following example shows a portion of the `OracleDrive10.2.SED` file:

   ```
   TargetName=C:\odrive\OracleDrive10.2.exe
   FriendlyName=Oracle Drive 10.2.0.0.0
   AppLaunched=ODUpgrade.exe
   PostInstallCmd=<None>
   AdminQuietInstCmd=
   UserQuietInstCmd=
   FILE0="ODriveSetup10.2.0.0.0.exe"
   FILE1="ODUpgrade.exe"
   FILE2="dotnetfx.exe"
   FILE3="odrive.ini"
   [SourceFiles]
   SourceFiles0=C:\odrive\binaries\
   SourceFiles1=C:\odrive\extra\
   [SourceFiles0]
   %FILE0%=
   %FILE1%=
   %FILE2%=
   [SourceFiles1]
   %FILE3%=
   ```

6. Use the IExpress utility to re-package the files into a self-extracting executable. To do this, open a command prompt and go to the location where the `SED` file is located, then run this command:

   ```
   iexpress /N OracleDrive10.2.SED
   ```

7. Copy the Oracle Drive executable to a location where users can download it. You can find the executable at the location you specified for `TargetName` in the `SED` file.

Installing Oracle Drive from the Client CD

If you choose not to set up the administrator-configured installation of Oracle Drive for your users, you can copy the installation files from the Oracle Drive client CD to a location where your users can download them. In order to install Oracle Drive, there must available disk space equivalent to twice the size of the install files

The following instructions explain how to install Oracle Drive from the client CD or from a posted location.

Note: If you install Oracle Drive on a computer that has firewall software running, such as the native Windows XP firewall, you may see a message similar to the following:

```
Windows Security Alert: To help protect your computer, Windows
Firewall has blocked some features of this program.  Do you want to
keep blocking this program? ODFWAgent.exe
```

If you see this message, select **Unblock** to allow Oracle Drive to run.

To install Oracle Drive:

1. On the Oracle Drive client CD, or from the location where the installation files have been posted, double-click the Oracle Drive executable.
2. If you are accessing the installation files from a remote location, in the File Download window, select **Run this program from its current location**, then click **Yes** in the warning dialog box.

   You can also download the installation program to your local hard drive and run it from there. After downloading, double-click the executable file to begin installation.
3. If you have a previous version of Oracle Drive installed, the installation wizard prompts you to uninstall the previous version first. You must close any browser windows you have open before proceeding.
4. Oracle Drive requires Microsoft .NET Framework 1.1. If you do not have Microsoft .NET Framework 1.1, the installation wizard will install it for you.
5. On the Choose Setup Language screen, select a language and click **OK**.
6. On the Welcome screen, click **Next**.
7. On the Destination Folder screen, accept the default installation directory, or click **Change** to select a different installation directory. Then, click **Next**.
8. On the Miscellaneous Options screen, choose whether to add a shortcut to Oracle Drive on your desktop, and whether you want Oracle Drive to start automatically when Windows starts. Then, click **Next**.
9. On the Ready to Install the Program screen, click **Install** to install Oracle Drive, or click **Back** to change any values that you entered.
10. On the InstallShield Wizard Completed screen, click **Finish**.
11. The Oracle Drive installer prompts you to restart your computer. Select **Yes** to restart your computer automatically, or select **No** and restart your computer manually.

For complete information about how to set up a WebDAV connection between Oracle Drive and Oracle Content DB, as well as information about how to use Oracle Drive, see the Oracle Drive Help.

5

Choosing Oracle Content DB Options

After you install and configure Oracle Content DB, you may want to customize your setup for a particular deployment scenario. For example, you may want to enable Oracle Records DB, integrate Oracle Content DB with an antivirus solution, or run the Oracle Content DB application on a different port number.

Additional options are covered elsewhere in this book. See the following references for more information:

- "Enabling FTP" on page 4-3
- "Enabling FTPS" on page 4-4
- "Creating Sites" on page 11-2
- "Setting Up an Administrator-Configured Installation of Oracle Drive" on page 4-8

This chapter provides information about the following topics:

- Setting Up Oracle Records DB
- Setting Up Antivirus Integration
- Managing Storage Options
- Integrating with Solutions for Records Management Retention
- Changing the Oracle Content DB Port Number
- Allowing Access to Oracle Content DB from Outside the Firewall
- Changing a Middle-Tier Host Name or IP Address
- Customizing the New User Orientation

Setting Up Oracle Records DB

Records management is the systematic and comprehensive control of the creation, capture, maintenance, filing, use, and disposition of records. Its goal is to ensure that records:

- Are authentic and reliable
- Can be retrieved when needed as quickly and efficiently as possible
- Are not destroyed prematurely or kept longer than required

Oracle Records Database (Oracle Records DB) is a records management application that ships with Oracle Content DB. It must be licensed separately.

When you install Oracle Content DB, Oracle Records DB is installed automatically, but the application is disabled by default. You can use the Application Server Control to enable Oracle Records DB. You can also choose to configure metrics related to Oracle Records DB.

User permissions related to Oracle Records DB are managed from the Oracle Content DB Web client. See *Oracle Content Database Application Administrator's Guide* for more information.

For information about how to use Oracle Records DB, see *Oracle Records Database Administrator's Guide*.

Enabling Oracle Records DB

Although the Oracle Records DB application is disabled, by default, after you install and configure Oracle Content DB, you can use the Application Server Control to enable Oracle Records DB.

To enable Oracle Records DB, you must first enable the Oracle Records DB OC4J instance (`OC4J_RM`), then activate the node configuration for the Oracle Records DB HTTP node. Finally, you must activate the Records DB Lifecycle Agent.

Note: You *must* activate the node configuration for the Oracle Records DB HTTP node to use Oracle Records DB. It is not enough to enable only the Oracle Records DB OC4J instance.

Enabling Oracle Records DB OC4J Instances

If you have multiple Oracle Content DB middle tiers on which you want to enable Oracle Records DB, you must connect to the Application Server Control on each middle tier to enable multiple Oracle Records DB OC4J instances.

To enable Oracle Records DB OC4J instances:

1. Connect to the Application Server Control and go to the Application Server Home page.
2. From the Application Server Home page, click **Enable/Disable Components**.
3. From the Disabled Components list, select **OC4J_RM** and click **Remove**. The selected component appears in the Enabled Components list.
4. Click **OK**.
5. Restart Oracle HTTP Server (**HTTP_Server**) from the Application Server Home page.
6. Repeat these steps for each Oracle Content DB middle tier on which you want to run Oracle Records DB.

Activating Oracle Records DB HTTP Node Configurations

You can activate all Oracle Records DB HTTP node configurations from one middle tier.

To activate Oracle Records DB HTTP node configurations:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Node Configurations**.
3. Click the name of the Oracle Records DB HTTP node for this middle tier. The name of the Oracle Records DB HTTP node appears in the following format: ***middle_tier_name*_RM_HTTP_Node**.

4. Select **Active** in the General section, then click **OK**.
5. If you have multiple middle tiers on which you want to enable Oracle Records DB, click the names of the Oracle Records DB HTTP nodes for the other middle tiers. On the Edit Node Configuration page for these nodes, select **Active**, then click **OK**.
6. Return to the Content DB Home page and start each Oracle Records DB HTTP node. To do this, select each **OC4J_RM** instance in the Processes list and click **Start**.

   Each Oracle Records DB HTTP node has the same display name (`OC4J_RM`). Use the Middle Tier column of the Processes table to distinguish between different Oracle Records DB HTTP nodes.
7. Select all **OC4J_Content** instances in the Processes list and click **Restart**. This step is necessary to enable records functionality in the Oracle Content DB Web client.
8. After you have at least one Oracle Records DB HTTP node running, you can access the Oracle Records DB application from any Web browser. The default URL is:

   ```
   http://hostname:port/rm
   ```

   Use the same host name and port as for the Oracle Content DB application. Use `https://` if you are using SSL.

Activating the Records DB Lifecycle Agent

The Records DB Lifecycle Agent runs on only one middle tier. You must activate this agent for Oracle Records DB to work properly.

See "Records DB Lifecycle Agent" on page E-15 for more information about this agent.

To activate the Records DB Lifecycle Agent:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Node Configurations**.
3. On the Node Configurations page, click the name of the regular node that runs the Records DB Lifecycle Agent.
4. In the Servers section, select **RmLifeCycleAgent** and click **Edit**.
5. Select **Active**, then click **OK**.
6. On the Edit Node page, click **OK**.
7. Return to the Content DB Home page and restart the node that corresponds to the node configuration you edited.

Configuring Metrics Related to Oracle Records DB

You can optionally choose to collect metrics related to Oracle Records DB Web application response time by configuring particular performance metrics on each middle tier. For more information about how to do this, see "Configuring Performance Metrics" on page 9-4.

Setting Up Antivirus Integration

Oracle Content DB integrates with a partner solution, the Symantec AntiVirus Scan Engine (SAVSE), to provide options to verify that content is virus free and to clean files that are infected.

After antivirus integration has been set up, files will be scanned for viruses whenever they are opened for read access, using the latest available virus definitions. The following files will be excluded from the scanning process:

- Files that are quarantined
- File formats (such as .doc) that are excluded by the administrator
- Files that have already been scanned using the current virus definitions

If a file is infected with a virus, it will be marked as quarantined, and users will not be able to open the file until it is repaired. Contents of the file will remain unreadable even if virus checking is disabled by the administrator.

The Virus Repair Agent is responsible for repair attempts and retrieving the latest virus definitions. Whenever the agent becomes active, it polls the SAVSE server for updated virus definitions, and then attempts to repair the quarantined files. The agent will not attempt to repair the following files:

- Files that have exceeded the maximum number of repair attempts
- Files that have already experienced repair attempts using the current virus definitions

The following sections describe how to set up virus checking in Oracle Content DB:

- Setting Up SAVSE
- Enabling Antivirus Functionality in Oracle Content DB
- Excluding Formats from Being Scanned
- Performance Implications of Scanning for Viruses

Setting Up SAVSE

SAVSE must be installed and configured properly to function with Oracle Content DB. The following options must be set:

- You must select ICAP as the communication protocol. No other protocols are supported.
- You must set the scan policy to Scan and Repair or Scan Only. If you choose Scan Only, no repair attempts will be made. The Scan and Delete and Scan, Repair or Delete options are not supported.
- You must enable the ICAP 403 response. This parameter cannot be set using the SAVSE administration tool; instead, it must be manually set in the SAVSE configuration file.

Enabling Antivirus Functionality in Oracle Content DB

After the SAVSE server has been installed and configured, you can enable antivirus functionality in Oracle Content DB. You can also change the maximum number of repair attempts for quarantined documents, and configure how often the Virus Repair Agent is activated. Use the Application Server Control to perform these tasks.

To enable antivirus functionality and set the maximum number of repair attempts:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Domain Properties**.
3. Click the **IFS.DOMAIN.ANTIVIRUS.Enabled** property, set the value to **true**, and click **OK**.

4. Click the **IFS.DOMAIN.ANTIVIRUS.Host** property, enter the host name or IP address of the computer where the SAVSE server is running, and click **OK**.
5. Click the **IFS.DOMAIN.ANTIVIRUS.MaxRepairAttempts** property, enter the number of times you want the Virus Scan Agent to attempt to repair a file, and click **OK**.
6. Click the **IFS.DOMAIN.ANTIVIRUS.Port** property, enter the value for the SAVSE listener port, and click **OK**.
7. Return to the Content DB Home page and click **Restart Domain**.

To configure how often the Virus Repair Agent becomes active:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Server Configurations**.
3. Click **VirusRepairAgentConfiguration**.
4. In the Properties section, click **IFS.SERVER.TIMER.ActivationPeriod**.
5. Change the **Value** as necessary.
6. On the Edit Property page, click **OK**.
7. On the Edit Server Configuration page, click **OK**.
8. Return to the Content DB Home page and restart the node that runs this agent.

Excluding Formats from Being Scanned

You can exclude formats from being scanned for viruses to improve system performance. For example, you may choose to only scan formats with a higher probability of being infected, such as .zip files. Use the Application Server Control to exclude formats from virus checking.

To exclude formats from being scanned:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Formats**.
3. Click the name of the format you want to exclude from virus scanning.
4. Select **Omitted From Antivirus Scan**.
5. Click **OK**.

Performance Implications of Scanning for Viruses

The performance of Oracle Content DB may be affected by enabling the virus checking option. The performance impact depends on the following factors:

- The frequency of virus definition updates made to the SAVSE service. Each time virus definitions are updated, *all* files that are opened (except for quarantined or excluded files) are scanned - none are excluded based on having already been scanned with these definitions, because the definitions are new.

  After a virus definition update, overall system performance will degrade initially, but will gradually return to normal as more files are scanned with the current virus definitions and are therefore excluded from subsequent scans.
- The size and frequency of use of the Oracle Content DB repository.
- The type and size of the data in the repository.

- The probability of the number of attempted reads on unique files. Since files will only be scanned the first time they are opened against the current definitions, the frequency of unique files will affect performance.
- The performance of the SAVSE service. This is the most significant performance factor.
- The number of files whose format has been excluded from scanning by the administrator. Excluding certain formats will reduce the number of scans and improve system performance.

Managing Storage Options

The Oracle Content DB storage management options provide support for both offline and near-line storage. In offline and near-line storage, content that is infrequently accessed is moved from expensive online media, such as a disk array, to a cheaper offline medium, such as tape. The metadata and search indexes are kept online and are readily available.

Oracle Content DB uses BFILEs to support offline and near-line storage. A BFILE is a read-only Oracle data type consisting of a directory object and a file name. Updating a document whose content is stored as a BFILE results in the content being reloaded from the external storage as a new binary large object (BLOB), where the modifications are made. The new content will be indexed, depending on its format. End users will be unaware of where their content is stored.

This section provides information about the following topics:

- Data Aging and Archiving
- Near-Line Storage for Records
- Specifying Storage Management Options

Data Aging and Archiving

Oracle Content DB provides both data aging and data archiving through BFILEs. Through data aging, content that has not been accessed for a specified interval can be automatically moved from a BLOB to a BFILE. Through data archiving, content in the **Archive** is automatically moved from a BLOB to a BFILE.

Content that has been moved to a BFILE is still accessible, and is visible as any content would be when users are browsing or searching.

BFILE aging and archiving are not enabled by default. Follow the instructions in the subsequent sections to set up BFILE aging and archiving:

- Setting Up Data Aging
- Setting Up Data Archiving

Setting Up Data Aging

Oracle Content DB is not set up for BFILE aging by default. To configure BFILE aging, you must first set domain properties that enable BFILE aging, then you must configure and activate the Content Agent. You can also specify storage management options.

To set domain properties that enable BFILE aging:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Domain Properties**.

3. Click **IFS.DOMAIN.BFILE.Enabled**, set the value to **true**, and click **OK**.
4. Click **IFS.DOMAIN.BFILE.AgingEnabled**, set the value to **true**, and click **OK**.
5. Return to the Content DB Home page and click **Restart Domain**.

To configure and activate the Content Agent:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Server Configurations**.
3. Click **ContentAgentConfiguration**.
4. Edit the server configuration properties as desired; see the Content Agent properties in Appendix E, "Server Configuration Properties" for more information about specific properties. In particular, you may want to edit **IFS.SERVER.AGENT.CONTENTAGENT.RetentionPeriod**; this property specifies the inactivity interval for files before they are moved to a BFILE.
5. Click **OK**.
6. Return to the Content DB Home page, and in the Administration section, click **Node Configurations**.
7. Click the name of the node configuration that corresponds to the node where you want to run the Content Agent.
8. On the Edit Node Configuration page, in the Servers section, click **ContentAgent**.
9. Select **Initially Started** and click **OK**.
10. On the Edit Node Configuration page, click **OK**.
11. Return to the Content DB Home page, select the node that corresponds to the node configuration you edited, and click **Restart**.

After you have set the domain properties for BFILE aging and configured the Content Agent, you can set storage management options as described in "Specifying Storage Management Options" on page 5-8.

Setting Up Data Archiving

Oracle Content DB is not set up for BFILE archiving by default. To configure BFILE archiving, you must set domain properties that enable BFILE archiving. You can also specify storage management options.

To set domain properties that enable BFILE archiving:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Domain Properties**.
3. Click **IFS.DOMAIN.BFILE.Enabled**, set the value to **true**, and click **OK**.
4. Click **IFS.DOMAIN.BFILE.ArchivingEnabled**, set the value to **true**, and click **OK**.
5. Return to the Content DB Home page and click **Restart Domain**.

After you have set the domain properties for BFILE archiving, you can set storage management options as described in "Specifying Storage Management Options" on page 5-8.

Near-Line Storage for Records

If you are using Oracle Records DB, you have the option of storing certain types of records using BFILEs. Near-line storage for records is not enabled by default; to enable this option, you must set a BFILE-related domain property and specify storage management options.

Setting Up Near-Line Storage for Records

To set the domain property that enables near-line records storage:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Domain Properties**.
3. Click **IFS.DOMAIN.BFILE.Enabled**, set the value to **true**, and click **OK**.
4. Return to the Content DB Home page and click **Restart Domain**.

After you have set the domain property to enable near-line storage for records, you can set storage management options as described in the following section.

Specifying Storage Management Options

You can change the default base path and policy for BFILE storage using the Application Server Control. These settings apply to all types of BFILE storage, including BFILE aging, BFILE archiving, and near-line storage for records.

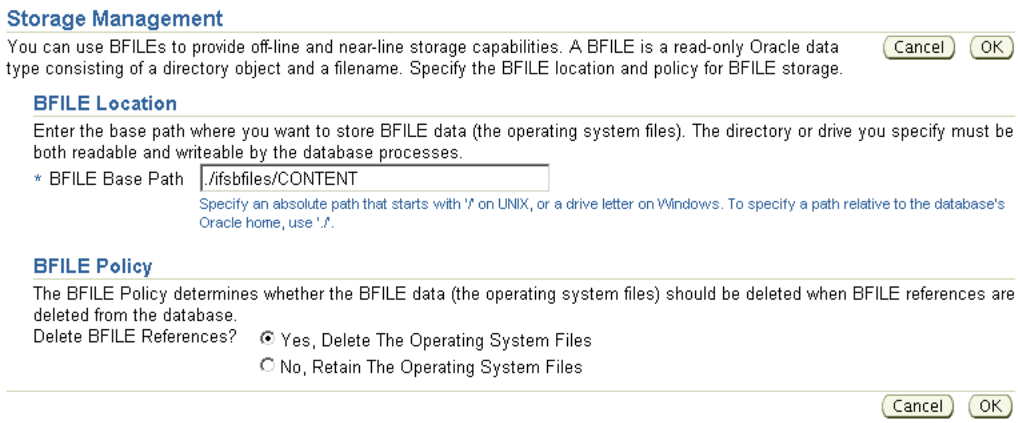
To specify storage management options:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Storage Management**.

   You will not be able to access the Storage Management page unless you have already set the **IFS.DOMAIN.BFILE.Enabled** property to **true**.

   Figure 5–1 shows the Storage Management page.

Figure 5–1 Storage Management Page



You can use BFILEs to provide off-line and near-line storage capabilities. A BFILE is a read-only Oracle data type consisting of a directory object and a filename. Specify the BFILE location and policy for BFILE storage.

BFILE Location

Enter the base path where you want to store BFILE data (the operating system files). The directory or drive you specify must be both readable and writeable by the database processes.

* BFILE Base Path: ./ifsbfiles/CONTENT

Specify an absolute path that starts with '/' on UNIX, or a drive letter on Windows. To specify a path relative to the database's Oracle home, use './'.

BFILE Policy

The BFILE Policy determines whether the BFILE data (the operating system files) should be deleted when BFILE references are deleted from the database.

Delete BFILE References?
● Yes, Delete The Operating System Files
○ No, Retain The Operating System Files

3. Change the **BFILE Base Path**. The default base path is:

   ORACLE_HOME/`ifsbfiles`/*content_db_schema*

   ORACLE_HOME refers to the database Oracle home on the database computer.

   Each BFILE has a relative path in addition to the base path. The relative path is:

   /*yyyy*/*dd*/*mm*/*hh*/*mm*/*ss*/`ifsbfile_id`

In the relative path, `ifsbfile_id` is the file naming pattern that associates a unique ID to each piece of content.

4. Change the **BFILE Policy**. This policy determines whether the operating system files should be deleted when the BFILE references are deleted from the database. If you are storing BFILEs on an optical device that does not permit deletion, you should specify that the operating system files should be retained.
5. Click **OK**.

Integrating with Solutions for Records Management Retention

Oracle Content DB supports integration with two records management retention solutions: Network Appliance SnapLock and EMC Centera. These retention storage solutions provide write once, read many (WORM) data permanence capabilities for records management and regulatory compliance requirements. The critical data becomes immutable, nonrewritable, and unremovable for a specified retention period.

You must license Oracle Records DB in order to use a retention storage solution with Oracle Content DB.

To integrate Oracle Content DB with a records management retention device, you must install and configure the hardware, either Network Appliance SnapLock or EMC Centera. Then, refer to the following sections for additional information about configuring Oracle Content DB for the appropriate retention device:

- Configuring Oracle Content DB for Network Appliance SnapLock
- Configuring Oracle Content DB for EMC Centera

Configuring Oracle Content DB for Network Appliance SnapLock

Follow the instructions in this section to configure Oracle Content DB for Network Appliance SnapLock integration. Before you begin, make sure that Oracle Records DB has been configured and that the Records DB Lifecycle Agent has been activated. See "Setting Up Oracle Records DB" on page 5-1 for more information.

This section contains the following topics:

- Configuring the Database Computer for Network Appliance SnapLock
- Configuring the Middle-Tier Computer for Network Appliance SnapLock

Configuring the Database Computer for Network Appliance SnapLock

Network Appliance SnapLock uses NFS to move data from the Oracle Content DB database to the retention storage device.

To configure the database computer on UNIX systems:

1. As the root user, perform an NFS mount to the SnapLock volume. Refer to the documentation for your operating system for optimum NFS mount point options.
2. In the mounted directory, create another directory. This new directory will be considered as the relative path to the SnapLock volume. The owner and group permissions on this new directory must be the same as that of the operating system user running the database.

To configure the database computer on Microsoft Windows systems:

1. On the database computer, install and configure an NFS client for Windows systems.

2. Ensure that the `pcnfsd` daemon process is running on the Network Appliance device. To start the `pcnfsd` process:

    a. Access the Web-based Network Appliance administration tool, `na_admin`, using the following URL:

    ```
    http://hostname/na_admin
    ```

    b. Click the **FilerView** icon.

    c. When prompted, provide the `na_admin` user name and password.

    d. Click **NFS** > **Configure** in the left navigation pane.

    e. Set **PCNFS Enabled** to **Yes**.

    f. Click **Apply**.

    Alternatively, you can telnet to the Network Appliance device and type the following command:

    ```
    options pcnfsd.enable on
    ```

3. Use the NFS client to map a drive to the SnapLock volume. This will cause the SnapLock volume to appear as a drive letter.

    Refer to the documentation for your NFS client for optimum NFS mount point options.

Configuring the Middle-Tier Computer for Network Appliance SnapLock

Perform the following steps on the middle tier that is running the Records DB Lifecycle Agent. To determine which middle tier is running this agent, use the Application Server Control to view each node to see where the agent is running.

Follow the steps in these sections to configure the middle tier:

- Installing the Network Appliance SnapLock Software
- Setting Domain Properties for Network Appliance SnapLock
- Specifying Credential Information for Network Appliance SnapLock

Installing the Network Appliance SnapLock Software

You must install the Network Appliance SnapLock software on the middle tier that is running the Records DB Lifecycle Agent. To do this, follow these steps:

1. Obtain the Network Appliance SnapLock software (version 1.5 or later), located in the Network Appliance `manageontap.jar` file. You can obtain this file from the Network Appliance NOW (NetApp on the Web) site at `http://now.netapp.com`.

    You must become a member of the NOW site by clicking the **New User Sign Up** link. There is no cost to join. Once you are a member, go to the following URL to download the software:

    ```
    http://now.netapp.com/NOW/download/tools/oraclecs_manageontap/
    ```

    Be sure to refer to the Network Appliance certification information to ensure that Network Appliance supports your operating system.

2. Copy the `manageontap.jar` file to the *ORACLE_HOME*`/content/lib` directory.

3. Modify the classpath in the following XML files to include the `manageontap.jar` file:

- `ORACLE_HOME/opmn/conf/opmn.xml`
- `ORACLE_HOME/j2ee/OC4J_Content/application-deployments/content/content/orion-web.xml`
- `ORACLE_HOME/j2ee/OC4J_RM/application-deployments/rm/rm/orion-web.xml`

Note: For more information about the Network Appliance software, refer to *Data ONTAP System Administration Guide* at the Network Appliance NOW site at `http://now.netapp.com`.

Setting Domain Properties for Network Appliance SnapLock

Use the Application Server Control Control to set domain properties related to Network Appliance SnapLock. To do this, follow these steps:

1. On the Content DB Home page, click **Domain Properties**.
2. Click **IFS.DOMAIN.RETENTION.StorageDevice**. You may need to move to the next page to find this property, or you can use the **Search** field.
3. In the **Value** field, select **SNAPLOCK** and click **OK**.
4. Click **IFS.DOMAIN.RETENTION.SNAPLOCK.Configuration**.
5. Click **HOST**.
6. In the **Value** field, specify the host name or IP address of the Network Appliance device and click **OK**.
7. Click **MOUNTPOINT**.
8. In the **Value** field, enter the absolute path where the Network Appliance is NFS-mounted on the database and click **OK**.

   If the database computer is running on Windows, you must enter a universal naming convention (UNC) path. For example, for a Filer called **snapserver** and a volume called **wormdrive**, you would enter the following path:

   ```
   \\\\snapserver\\wormdrive
   ```

   Because the backslash (\) is a common escape character, you must add an additional backslash to each backslash in the path. This means that you must enter four backslashes at the beginning of the path.
9. Click **PORT**.
10. In the **Value** field, enter the port used to communicate with the Network Appliance device through HTTP and click **OK**. The default port is 80.
11. Click **RELATIVEPATH**.
12. In the **Value** field, specify the relative path to the NFS mount point where content should be stored and click **OK**.

    If the database computer is running on Windows, you must enter a universal naming convention (UNC) path. Because the backslash (\) is a common escape character, you must add an additional backslash to each backslash in the path.
13. Click **SNAPLOCKEXPORTPATH**.

14. In the **Value** field, specify the absolute path of the NFS-exported volume and click **OK**.
15. On the Edit Domain Property page, click **OK**.

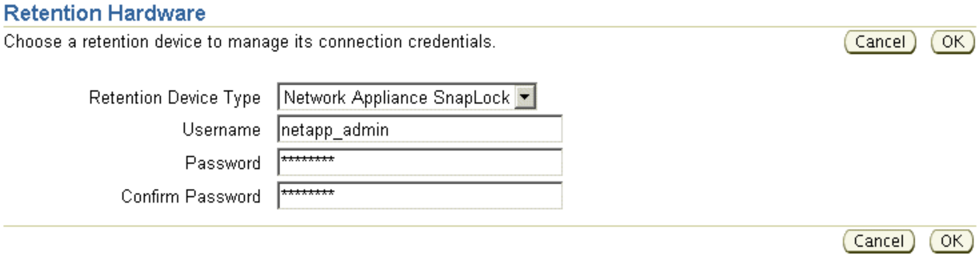
Specifying Credential Information for Network Appliance SnapLock

Use the Application Server Control to specify credential information for Network Appliance SnapLock. To do this, follow these steps:

1. On the Content DB Home page, click **Retention Hardware**.

   Figure 5–2 shows the Retention Hardware page.

Figure 5–2 Retention Hardware Page



Retention Hardware

Choose a retention device to manage its connection credentials.

Retention Device Type: Network Appliance SnapLock
Username: netapp_admin
Password: ********
Confirm Password: ********

2. In the **Retention Device Type** field, select **Network Appliance SnapLock**.
3. Enter a **Username** for Network Appliance SnapLock. You must provide a user name created in Network Appliance SnapLock; do not provide an Oracle Content DB user name.
4. Enter a corresponding **Password** for Network Appliance SnapLock, and confirm it in the **Confirm Password** field.
5. Click **OK**.
6. Return to the Content DB Home page and click **Restart Domain**.

Configuring Oracle Content DB for EMC Centera

Follow the instructions in this section to configure Oracle Content DB for EMC Centera integration. Before you begin, make sure that Oracle Records DB has been configured and that the Records DB Lifecycle Agent has been activated. See "Setting Up Oracle Records DB" on page 5-1 for more information.

You should perform the steps in the following sections on the middle tier that is running the Records DB Lifecycle Agent. To determine which middle tier is running this agent, use the Application Server Control to view each node to see where the agent is running

This section contains the following topics:

- Installing the EMC Centera Software
- Setting Domain Properties for EMC Centera
- Specifying Credential Information for EMC Centera

Installing the EMC Centera Software

You must install the EMC Centera software on the middle tier that is running the Records DB Lifecycle Agent. To do this, follow these steps:

1. Download EMC Centera 3.1 Patch 1 SDK or later from Oracle*MetaLink* at `http://metalink.oracle.com`. To find the SDK on Oracle*MetaLink*, search for patch number 5072277.

   This SDK contains the necessary .jar and library files. Follow the instructions in the readme to install the software.

2. Modify the classpath in the following XML files to include the `FPLibrary.jar` file:

   - `ORACLE_HOME/opmn/conf/opmn.xml`
   - `ORACLE_HOME/j2ee/OC4J_Content/application-deployments/content/content/orion-web.xml`
   - `ORACLE_HOME/j2ee/OC4J_RM/application-deployments/rm/rm/orion-web.xml`

3. In `ORACLE_HOME/opmn/conf/opmn.xml`, include the directory that contains the libraries in the appropriate path variable for the node, `OC4J_Content`, and `OC4J_RM`. This variable is called `LD_LIBRARY_PATH` on Linux and Solaris, PATH on Windows, `SHLIB_PATH` on HPUX, and `LIBPATH` on AIX. For example, on Linux, include the following entry:

```
<environment>
  <variable id="$LD_LIBRARY_PATH" value "$LD_LIBRARY_PATH:absolute_path_to_
Centera_lib_directory"/>
</environment>
```

   An example path on Linux could be:

```
/usr/local/centera31/lib
```

> **Note:** If `opmn.xml` does not include an `<environment>` entry for the variable for your platform, you must create one.

Setting Domain Properties for EMC Centera

Use the Application Server Control to set domain properties related to EMC Centera. To do this, follow these steps:

1. On the Content DB Home page, click **Domain Properties**.
2. Click **IFS.DOMAIN.RETENTION.StorageDevice**. You may need to move to the next page to find this property, or you can use the **Search** field.
3. In the **Value** field, select **CENTERA** and click **OK**.
4. Click **IFS.DOMAIN.RETENTION.CENTERA.Configuration**.
5. Click **ADDRESSLIST**.
6. In the **Value** field, enter the comma-delimited IP addresses of the EMC retention clusters and click **OK**.
7. On the Edit Domain Property page, click **OK**.

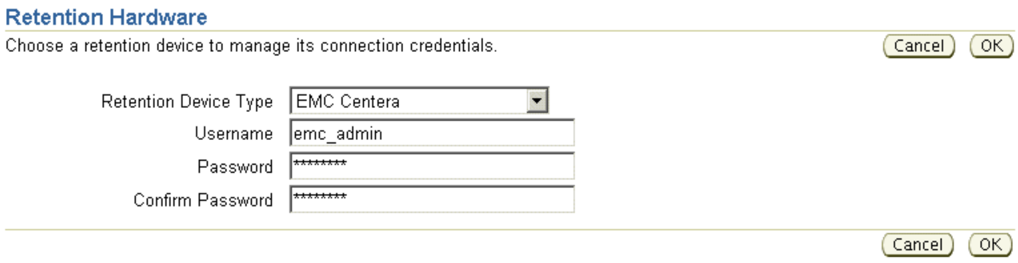
Specifying Credential Information for EMC Centera

Use the Application Server Control to specify credential information for EMC Centera. To do this, follow these steps:

1. From the Content DB Home page, click **Retention Hardware**.

Figure 5–3 shows the Retention Hardware page.

Figure 5–3 Retention Hardware Page



Retention Hardware

Choose a retention device to manage its connection credentials.

Retention Device Type: EMC Centera
Username: emc_admin
Password: ********
Confirm Password: ********

2. In the **Retention Device Type** field, select **EMC Centera**.
3. Enter a **Username** for EMC Centera. You must provide a user name created in EMC Centera; do not provide an Oracle Content DB user name.
4. Enter a corresponding **Password** for EMC Centera, and confirm it in the **Confirm Password** field.
5. Click **OK**.
6. Return to the Content DB Home page and click **Restart Domain**.

Changing the Oracle Content DB Port Number

If you want to change the Oracle Content DB application port to a different port number, perform the tasks listed in the following sections:

- Changing the Port Number in Oracle HTTP Server
- Changing the Port Number in OracleAS Web Cache
- Registering the New Port with OracleAS Single Sign-On
- Changing the Port Number in Oracle Content DB
- Updating Metric Configuration URLs

Changing the Port Number in Oracle HTTP Server

Use the Application Server Control to change the port number in Oracle HTTP Server.

1. From the Application Server Home page, click **HTTP_Server**.
2. Click **Administration**.
3. Click **Server Properties**.
4. In the Listening Addresses and Ports section, change the **Default Port** to the desired port number.
5. Click **Apply**.
6. On the Confirmation page, click **Yes** to restart Oracle HTTP Server.

Changing the Port Number in OracleAS Web Cache

If OracleAS Web Cache is enabled, you must change the port number in OracleAS Web Cache using the Application Server Control. To do this, follow these steps:

1. From the Application Server Home page, choose **Web Cache**.

2. Click the **Administration** tab, then click **Ports** in the Properties - Web Cache section.
3. Change the appropriate port number in the Listen Ports section, then click **OK**.
4. Return to the Web Cache Home page and click **Restart**.

Registering the New Port with OracleAS Single Sign-On

After you change the port number in Oracle HTTP Server, you must register the new port with OracleAS Single Sign-On. To do this, run the single sign-on registration tool, then restart Oracle HTTP Server. See "Registering mod_osso" in *Oracle Application Server Single Sign-On Administrator's Guide* for more information.

Changing the Port Number in Oracle Content DB

Use the Application Server Control to update the Oracle Content DB Application Port domain property and restart the Oracle Content DB OC4J instance:

1. From the Content DB Home page, in the Administration section, click **Domain Properties**.
2. On the Domain Properties page, click **IFS.DOMAIN.APPLICATION.ApplicationPort**. You may need to move to the next page to find this domain property, or you can use the **Search** field.
3. On the Edit page, enter the new port number in the **Value** field and click **OK**. If you are using a load balancer with multiple Oracle Content DB middle tiers, enter the load balancer port.
4. Return to the Content DB Home page.
5. Select **OC4J_Content** and click **Restart**. If you are using Oracle Records DB, you also need to restart **OC4J_RM**.

Updating Metric Configuration URLs

You also need to update the port number for any affected Web application response time metrics. To do this, update the affected URLs on the Metric Configuration page in the Application Server Control. See "Configuring Performance Metrics" on page 9-4 for more information.

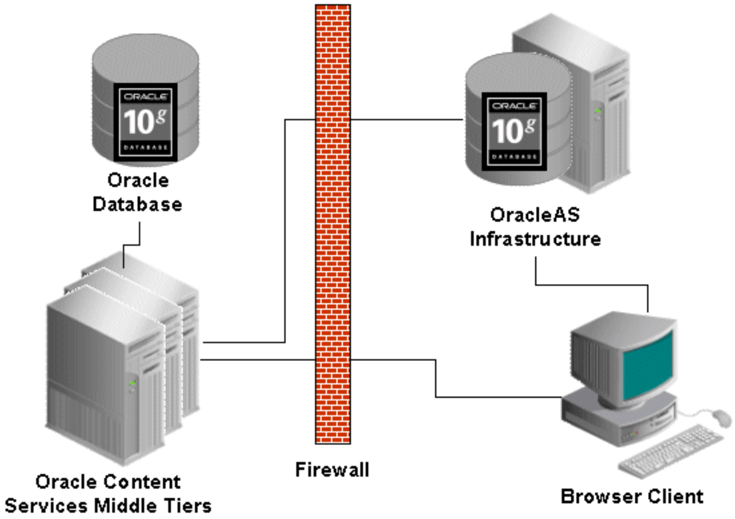
Allowing Access to Oracle Content DB from Outside the Firewall

You can set up Oracle Content DB so that users outside the firewall can have access. To do this, follow these steps:

1. **Open ports.** Disable the firewall for the following ports:
   - Oracle Content DB domain ports (node manager, node controller)
   - Database listener port (typically 1521)
   - Apache port (Oracle HTTP Server port)
   - Oracle Internet Directory ports (if Oracle Internet Directory is running inside the firewall)
   - Load balancer port (if you use a load balancer)
2. **Set firewall timeout periods.** You must set the operating system parameter `TCP_keepalive` to 120 minutes.

Figure 5–4 shows a possible firewall scenario with the database and middle tiers inside the firewall, and with OracleAS Infrastructure outside the firewall.

Figure 5–4 Sample Firewall Configuration



Changing a Middle-Tier Host Name or IP Address

You can run a script to change the host name or IP address of a middle-tier host in Oracle Content DB. You can only run the script if you have a multiple-computer deployment of Oracle Content DB. In other words, you can only run the script if your middle tier does not run on the same host as Oracle Database or Oracle Internet Directory.

To change the host name or IP address of your middle tier:

1. Shut down all middle-tier processes.

   These processes may include regular nodes, HTTP nodes (OC4J_Content and OC4J_RM), and the Application Server Control. See "Starting and Stopping the Oracle Content DB Domain" on page 7-1 for more information.

2. Change the host name or IP address on your middle-tier computer.

3. Change the host name or IP address for all of your other Oracle Application Server components. For information about how to do this, see *Oracle Application Server Administrator's Guide*.

4. Run the Oracle Content DB script `changehostname`, located in the following directory:

   ```
   ORACLE_HOME/content/bin
   ```

   Specify the old host name or IP address and the new host name or IP address as arguments. For example:

   ```
   changehostname old_host_name new_host_name
   ```

   or

   ```
   change hostname old_ip_address new_ip_address
   ```

If you need to change both the host name and the IP address, you must run the script twice, once to change the host name and once to change the IP address.

Note: You can view log information for this script in the `changehostname.log` file, located in:

`ORACLE_HOME``/content/log`

---

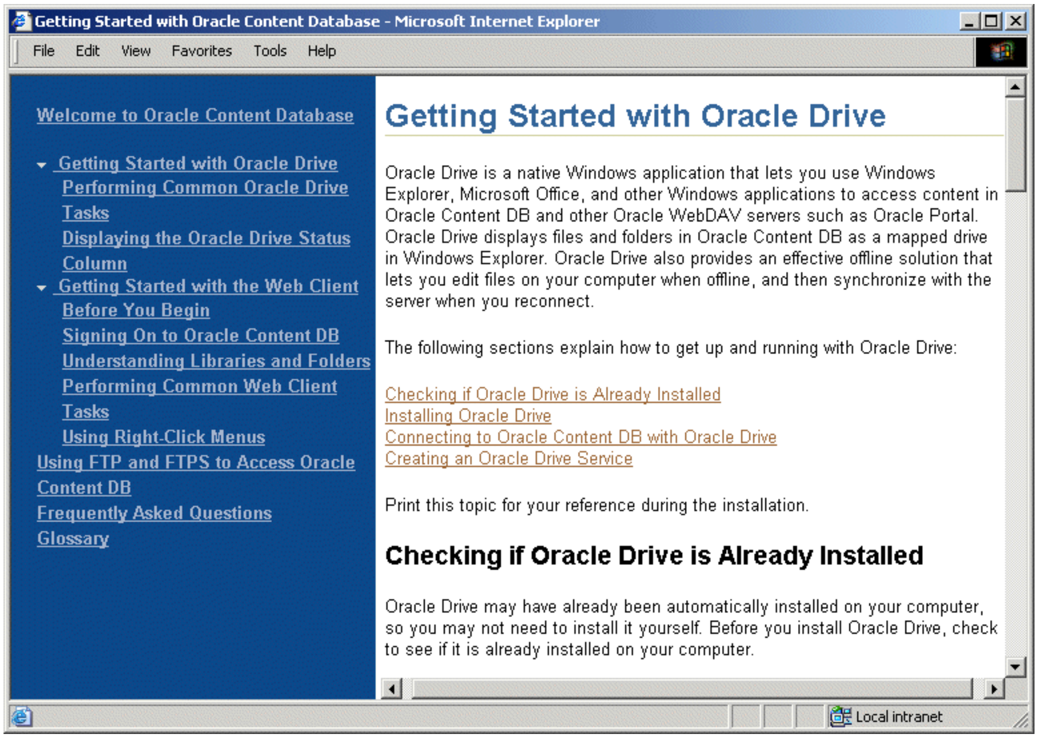
5. Start all middle-tier processes. See "Starting and Stopping the Oracle Content DB Domain" on page 7-1 for more information.

Customizing the New User Orientation

Oracle Content DB comes with a New User Orientation, a set of customizable help pages that users can access from the Oracle Content DB launch page. These pages provide valuable information, such as how to sign on to the Web client and how to get started with Oracle Drive, that can help new users get started with Oracle Content DB. The New User Orientation is only available in English.

Figure 5–5 shows the New User Orientation.

Figure 5–5 Oracle Content DB New User Orientation


Getting Started with Oracle Content Database - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Local intranet

Welcome to Oracle Content Database

- Getting Started with Oracle Drive
  - Performing Common Oracle Drive Tasks
  - Displaying the Oracle Drive Status Column
- Getting Started with the Web Client
  - Before You Begin
  - Signing On to Oracle Content DB
  - Understanding Libraries and Folders
  - Performing Common Web Client Tasks
  - Using Right-Click Menus

Using FTP and FTPS to Access Oracle Content DB

Frequently Asked Questions

Glossary

Getting Started with Oracle Drive

Oracle Drive is a native Windows application that lets you use Windows Explorer, Microsoft Office, and other Windows applications to access content in Oracle Content DB and other Oracle WebDAV servers such as Oracle Portal. Oracle Drive displays files and folders in Oracle Content DB as a mapped drive in Windows Explorer. Oracle Drive also provides an effective offline solution that lets you edit files on your computer when offline, and then synchronize with the server when you reconnect.

The following sections explain how to get up and running with Oracle Drive:

Checking if Oracle Drive is Already Installed
Installing Oracle Drive
Connecting to Oracle Content DB with Oracle Drive
Creating an Oracle Drive Service

Print this topic for your reference during the installation.

Checking if Oracle Drive is Already Installed

Oracle Drive may have already been automatically installed on your computer, so you may not need to install it yourself. Before you install Oracle Drive, check to see if it is already installed on your computer.

You can customize the HTML pages to make the information more useful for your users. For example, the topic called Signing On to Oracle Content DB includes the following text:

"Open the Oracle Content DB URL in your Web browser. If you don't know the URL, ask your administrator."

You can replace the value for "the Oracle Content DB URL" with the actual URL (for example, `http://`*`content_db_host_name`*`:`*`port`*`/content`).

You can replace any text in the New User Orientation help files. However, text that is especially appropriate for customization is highlighted in red.

The New User Orientation pages are located on each middle tier, in the following directory:

```
ORACLE_HOME/Apache/Apache/htdocs/eudp/
```

Then main entry point for the New User Orientation help files is index.html.

When you update HTML files in the New User Orientation, make sure to update the files on each middle tier.

6

Using Custom BPEL Workflows in Oracle Content DB

You can define custom BPEL workflow processes in **Oracle BPEL Process Manager**, and then register them in Oracle Content DB. The custom BPEL workflow processes are managed in Oracle BPEL Process Manager.

Note: Oracle Content DB comes with two default workflow processes, Parallel Vote and Serial Approval. Oracle Content DB uses **Oracle Workflow** to manage these default workflow processes. Oracle Workflow is configured and integrated with Oracle Content DB during Oracle Content DB configuration.

This chapter provides information about the following topics:

- About Custom Workflows
- Creating Custom Workflows in Oracle BPEL Process Manager
- Registering Custom Workflows with Oracle Content DB
- Deleting Custom Workflows from Oracle Content DB

About Custom Workflows

Custom workflows can be created in Oracle BPEL Process Manager, an Oracle product that provides a framework for designing, deploying, monitoring, and administering processes based on BPEL standards. Custom workflows are only available to the default Site in Oracle Content DB; additional Sites cannot use custom workflows.

After you have created a custom workflow in Oracle BPEL Process Manager, you can use the Application Server Control to register the workflow in Oracle Content DB. You must provide detailed information about the workflow, including the names of the launch event and cancel event, as well as specific parameters that are used in the workflow. Custom workflows are disabled by default; before you can access the Custom Workflow pages in the Application Server Control, you must set the `IFS.DOMAIN.WORKFLOW.BPEL.CreationEnabled` domain property to true.

Custom workflows can be blocking or nonblocking. A blocking workflow is one that requires an action for it to complete. For example, you can create a blocking workflow to handle document approval for publication: action on the part of the approvers is required before a document is published. An example of a nonblocking workflow is one that handles sending out notifications for published documents; in this case, a document can be published without waiting for the notifications to be sent.

About BPEL

The Business Process Execution Language (BPEL) is an XML-based language for enabling task-sharing across multiple enterprises using a combination of Web services. BPEL is based on the XML Schema, Simple Object Access Protocol (SOAP), and Web Services Description Language (WSDL). Using BPEL, you design a business process that integrates a series of discrete services into an end-to-end process flow. For more information about BPEL and Oracle BPEL Process Manager, see *Oracle BPEL Process Manager Developer's Guide*.

Creating Custom Workflows in Oracle BPEL Process Manager

For information about using Oracle BPEL Process Manager, see *Oracle BPEL Process Manager Developer's Guide*. For information about creating custom workflows for use with Oracle Content DB, see the Oracle Content DB developer documentation.

Registering Custom Workflows with Oracle Content DB

After the custom workflow has been created in Oracle BPEL Process Manager, you can register the custom workflow with Oracle Content DB using the Application Server Control. Before you can register the workflow, you must first enable BPEL workflow creation by setting the `IFS.DOMAIN.WORKFLOW.BPEL.CreationEnabled` domain property to true.

Enabling BPEL Workflow Creation in Oracle Content DB

To enable BPEL workflow creation in Oracle Content DB:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Domain Properties**.
3. Click **IFS.DOMAIN.WORKFLOW.BPEL.CreationEnabled**. You may need to move to the next page to find this property, or you can use the **Search** field.
4. Set the **Value** to true.
5. Click **OK**.
6. Return to the Content DB Home page and click **Restart Domain**.

Registering Custom Workflows

To register custom workflows in Oracle Content DB:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Custom Workflows**. You cannot access the custom workflow pages unless you have enabled BPEL workflow creation in Oracle Content DB.
3. Click **Register Workflow**.
4. Enter a name for the workflow. The name you provide must match the name of the workflow you created in Oracle BPEL Process Manager.
5. Enter a description of the workflow (optional).
6. Enter the **Launch Event** for the workflow. The event you provide must match the name of the corresponding Partner Link Correlation ID in Oracle BPEL Process Manager. The Launch Event cannot exceed 30 characters.

7. Enter the **Cancel Event** for the workflow. If you have a corresponding Partner Link Correlation ID in Oracle BPEL Process Manager, the event you provide must match the name of the Correlation ID. The Cancel Event cannot exceed 30 characters.

   Typically, the Cancel Event is not used. If this is the case, you can provide any string for this field (for example, CANCEL_MY_WORKFLOW).

8. Select **Blocking** if this workflow is a blocking workflow. A blocking workflow is one that requires an action for it to complete.
9. Select **Approvers Required** if this workflow requires approvers.
10. Click **Add** to add parameters for this workflow.
11. On the Register Workflow - Add Parameter page, specify information for the parameter you want to add:
    - **Name:** The name you provide must match the name of the parameter in Oracle BPEL Process Manager. The parameter name cannot exceed 30 characters.
    - **Description:** Enter an optional description of the parameter.
    - **Fixed Value:** Select this option if you do not want to allow changes to this parameter after the workflow has been created.
    - **Required:** Select this option if this parameter is required for the workflow to complete.
    - **Type:** Select one of the following type options for this parameter:
      - String
      - Boolean
      - Integer Number Range
      - String Enumeration
      - Date
      - Decimal Number Range
      - Path
      - Time Period
      - User/Group

      If you select **Integer Number Range**, **Decimal Number Range**, or **Time Period**, you can optionally specify a minimum and maximum value for this parameter. If you select **String Enumeration**, you must specify values for this parameter. To do this, specify a value and click **Add**. You can manage the list of enumerated values by using the arrows provided to alter the order of the list. You can remove values by clicking **Remove**.
12. Click **OK** on the Register Workflow - Add Parameter page.
13. Optionally, provide a default value for the parameter by specifying a value in the **Default Value** column of the Parameters table. If you selected **Fixed Value** for this parameter, you must provide a default value. Note the following:
    - To specify a default for a Date type parameter, click the calendar icon to ensure that the date you specify appears in the correct format (MM/dd/yyyy).

- For a Path type parameter, you must supply a valid Oracle Content DB path (for example, `/mysite/mylibrary/myfolder`).
- For a User/Group type parameter, you must supply a valid Oracle Content DB user or group name.

14. Repeat Steps 10 through 13 to add additional parameters as needed. You can modify parameters that you have already added by clicking the parameter name.
15. Click **OK** on the Register Workflow page.

You cannot edit a registered workflow. If you need to make any changes, you must delete the custom workflow, then register it again.

Deleting Custom Workflows from Oracle Content DB

You can use the Application Server Control to delete custom workflows. If any folder or Library in Oracle Content DB has been configured to use a particular custom workflow, the custom workflow cannot be deleted.

To delete custom workflows:

1. Connect to the Application Server Control and navigate to the Content DB Home page.
2. In the Administration section, click **Custom Workflows**. You cannot access the custom workflow pages unless you have enabled BPEL workflow creation in Oracle Content DB.
3. Select the workflow you want to delete and click **Delete**.
4. Click **OK** on the warning page. The workflow will be deleted as soon as the last active workflow completes.

7

Managing Oracle Content DB Processes

You can use the Application Server Control to manage Oracle Content DB processes, including starting and stopping the Oracle Content DB domain, starting and stopping servers, and managing nodes. You can also manage Oracle Content DB processes from the command line using the `opmnctl` utility. To manage Oracle Content DB using the Application Server Control or `opmnctl`, OPMN must be started on all middle tiers.

This chapter provides information about the following topics:

About the Oracle Content DB Domain

An Oracle Content DB **domain** is a logical grouping of Oracle Content DB nodes and an Oracle Database instance that contains the Oracle Content DB data.

The Oracle Content DB software runs as a set of middle-tier processes, called **nodes**. Oracle Content DB node processes manage one or more **services**, **agents**, and **protocol** servers.

Each node runs on a particular middle tier, or in other words, within a particular Oracle home. You can have multiple middle tiers on the same computer. Although the nodes of a domain are often split across a set of middle tiers, a single middle tier can have more than one Oracle Content DB node.

There are two types of nodes: **regular nodes** and **HTTP nodes**. Each HTTP node runs as part of an **OC4J** process. You cannot have more than two HTTP nodes on a single middle tier: one to support the Oracle Content DB application and one to support the Oracle Records DB application. The OC4J instance for the Oracle Content DB application is `OC4J_Content`, while the OC4J instance for the Oracle Records DB application is `OC4J_RM`.

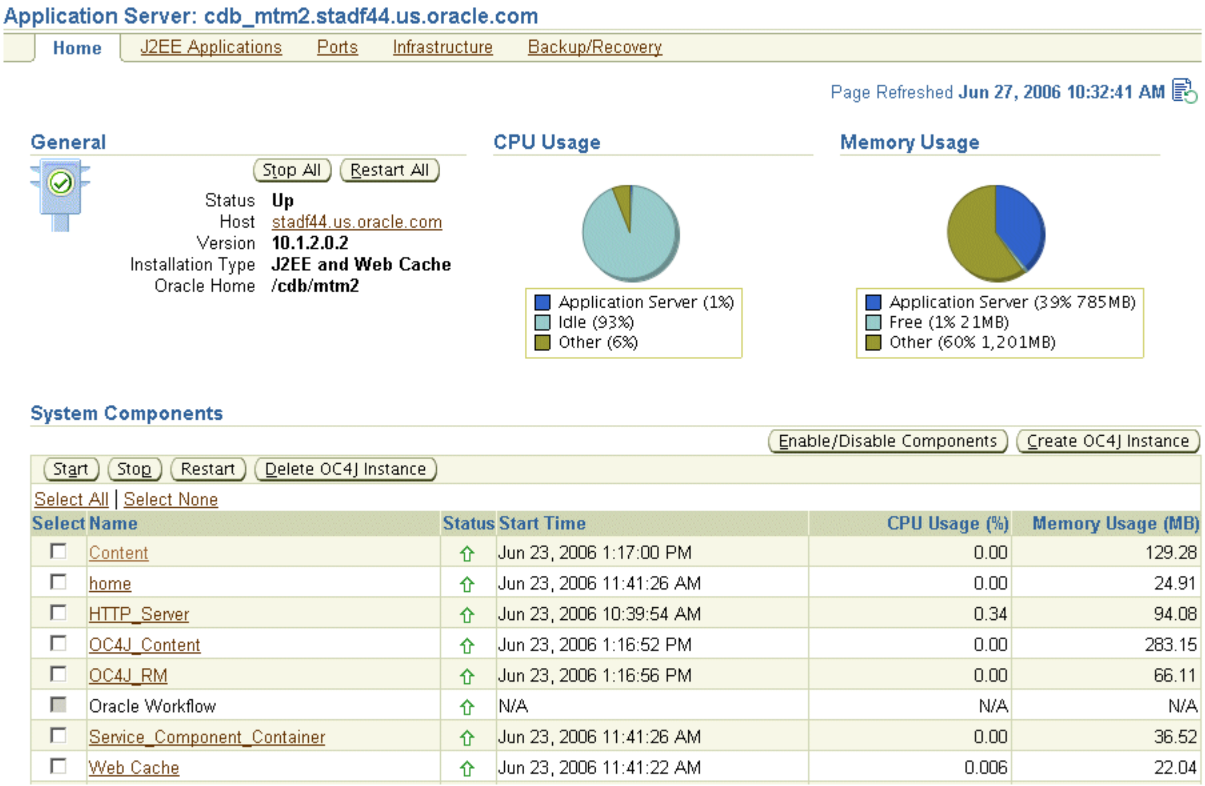
Starting and Stopping the Oracle Content DB Domain

You can start and stop the domain using the Application Server Control. Even if your domain is distributed across multiple middle tiers, you can start and stop the domain from a single middle tier.

1. From the Application Server Home page, click the name of the Oracle Content DB domain. Oracle Content DB domain targets typically appear as **Content**.

   Figure 7–1 shows the Application Server Home page.

Figure 7–1 Application Server Home Page



Application Server: cdb_mtm2.stadf44.us.oracle.com

Page Refreshed Jun 27, 2006 10:32:41 AM

Status **Up**
Host stadf44.us.oracle.com
Version **10.1.2.0.2**
Installation Type **J2EE and Web Cache**
Oracle Home **/cdb/mtm2**

CPU Usage:
🟦 Application Server (1%)
▨ Idle (93%)
▨ Other (6%)

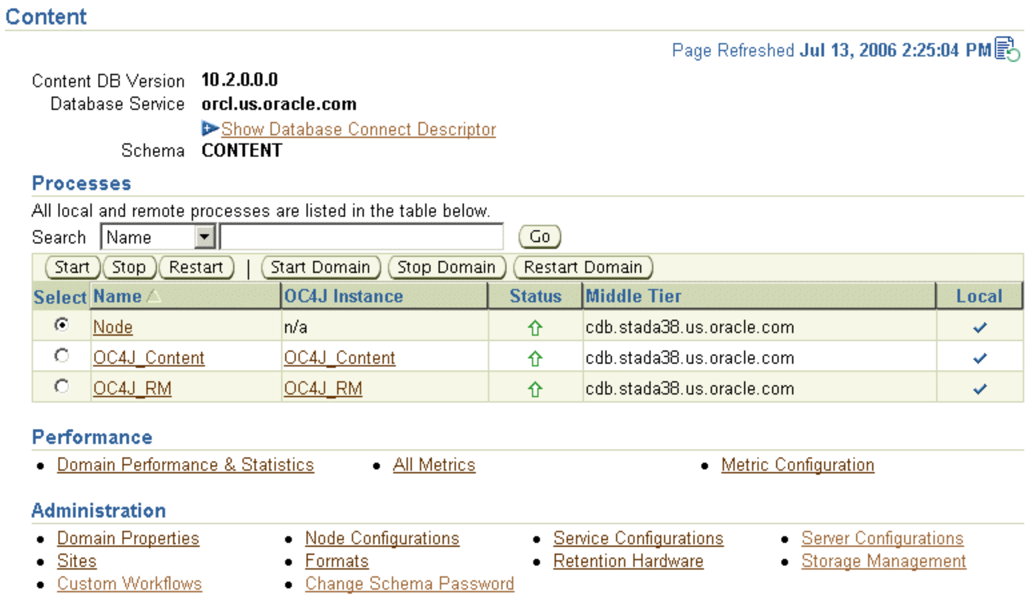
Memory Usage:
🟦 Application Server (39% 785MB)
▨ Free (1% 21MB)
▨ Other (60% 1,201MB)

Select	Name	Status	Start Time	CPU Usage (%)	Memory Usage (MB)
☐	Content	⇧	Jun 23, 2006 1:17:00 PM	0.00	129.28
☐	home	⇧	Jun 23, 2006 11:41:26 AM	0.00	24.91
☐	HTTP_Server	⇧	Jun 23, 2006 10:39:54 AM	0.34	94.08
☐	OC4J_Content	⇧	Jun 23, 2006 1:16:52 PM	0.00	283.15
☐	OC4J_RM	⇧	Jun 23, 2006 1:16:56 PM	0.00	66.11
☐	Oracle Workflow	⇧	N/A	N/A	N/A
☐	Service_Component_Container	⇧	Jun 23, 2006 11:41:26 AM	0.00	36.52
☐	Web Cache	⇧	Jun 23, 2006 11:41:22 AM	0.006	22.04

2. The Content DB Home page appears, showing the status of the set of nodes that belong to the domain. A green Up arrow in the Status column means the process is running.

   Figure 7–2 shows the Content DB Home page.

Figure 7–2 Content DB Home Page



Content

Page Refreshed **Jul 13, 2006 2:25:04 PM**

Content DB Version **10.2.0.0.0**
Database Service **orcl.us.oracle.com**
Show Database Connect Descriptor
Schema **CONTENT**

Processes

All local and remote processes are listed in the table below.

Select	Name	OC4J Instance	Status	Middle Tier	Local
●	Node	n/a	⇧	cdb.stada38.us.oracle.com	✓
○	OC4J_Content	OC4J_Content	⇧	cdb.stada38.us.oracle.com	✓
○	OC4J_RM	OC4J_RM	⇧	cdb.stada38.us.oracle.com	✓

Performance

- Domain Performance & Statistics
- All Metrics
- Metric Configuration

Administration

- Domain Properties
- Sites
- Custom Workflows
- Node Configurations
- Formats
- Change Schema Password
- Service Configurations
- Retention Hardware
- Server Configurations
- Storage Management

3. Start, stop, or restart the domain, as follows:
   - To start the Oracle Content DB domain, click **Start Domain**. The entire domain is started across all middle tiers, including all regular nodes and all HTTP nodes. Processes that are already running are not affected.
   - To restart the Oracle Content DB domain, click **Restart Domain**, then click **Yes** on the Warning page. The entire domain is restarted across all middle tiers, including all regular nodes and all HTTP nodes. Only those processes that are running are affected; processes that are not running will not be started.
   - To stop the Oracle Content DB domain, click **Stop Domain**, then click **Yes** on the Warning page. The entire domain is stopped across all middle tiers, including all regular nodes and all HTTP nodes.

     If you are performing scheduled maintenance and want to stop one middle tier at a time, do not click **Stop Domain**. Instead, start and stop individual domain processes, as follows:
   - To start, stop, or restart individual processes, such as regular nodes or HTTP nodes, select the appropriate process and click **Start**, **Stop**, or **Restart**. You can start, stop, or restart nodes that are on the local middle tier, or on remote middle tiers.

Using the Application Server Home Page to Start and Stop Oracle Content DB

You can start, stop, and restart Oracle Content DB from the Application Server Home page. Because the Application Server Home page only shows processes for the current middle tier, you need to log in to all your middle tiers separately to manage an Oracle Content DB deployment distributed across multiple middle tiers.

The Content DB Home page lets you see all Oracle Content DB processes across all middle tiers. In addition, each node process is listed separately on the Content DB Home page, providing you with maximum flexibility.

To start, stop, or restart Oracle Content DB from the Application Server Home page, select the domain display name (typically **Content**) and click **Start**, **Stop**, or **Restart**.

Managing Nodes at Run Time

You can use the Application Server Control to start, stop, and restart nodes, as well as modify run-time node properties and deactivate nodes.

You can also use the `opmnctl` utility to start, stop, and restart nodes, as well as check node status; see "Managing Oracle Content DB from the Command Line" on page 7-17 for more information.

This section contains the following topics:

- Starting, Stopping, and Restarting Nodes
- Modifying Nodes at Run Time
- Deactivating Nodes

Starting, Stopping, and Restarting Nodes

You can start, stop, and restart nodes using the Application Server Control. Even if your nodes are distributed across multiple middle tiers, you can start, stop, and restart them from a single middle tier, regardless of where the nodes are located.

If a node fails to start, stop, or restart, check the node logs for more information. Click **Logs** in the upper right corner of any Application Server Control page to search for and view node logs.

Starting Nodes

To start a regular node or HTTP node using the Application Server Control:

1. On the Content DB Home page, in the Processes section, select the node you want to start.
2. Click **Start**. The Status column displays a green arrow pointing up, indicating that the node is up.

Stopping Nodes

To stop a regular node or HTTP node using the Application Server Control:

1. On the Content DB Home page, in the Processes section, select the node you want to stop.
2. Click **Stop**.
3. On the Warning page, click **Yes** to stop the node. The Status column displays a red arrow pointing down, indicating that the node is down.

Restarting Nodes

You can only restart nodes that are already started.

To restart a regular node or HTTP node using the Application Server Control:

1. On the Content DB Home page, in the Processes section, select the node you want to restart.
2. Click **Restart**. The node is stopped, then started again.

Modifying Nodes at Run Time

You can make run-time changes to nodes, such as configuring loggers for the node log, changing the service used by the node, or changing servers. Changes made at run time are lost when the node is restarted. If you want to make permanent changes, modify the **node configuration** for the node and then restart the node.

To modify a node at run time using the Application Server Control:

1. On the Content DB Home page, in the Processes section, click the name of the node you want to modify. The Node page appears.
2. In the Logging section, you can configure loggers for this node. See "Configuring Node Loggers" on page 8-12 for more information.
3. In the Services section, you can create, modify, or delete services for this node. See "Managing Services at Run Time" on page 7-5 for more information.
4. In the Servers section, you can create, modify, or delete servers for this node. See "Managing Servers at Run Time" on page 7-12 for more information.

Deactivating Nodes

As an alternative to deleting a node configuration, consider making a node inactive instead. This option lets you keep the configuration information, and you can activate the node later.

Typically, you only deactivate nodes that are local to the current middle tier. In rare cases, however, such as when an middle tier fails, you may need to deactivate a node on a remote middle tier. Although nodes that were deactivated from remote middle tiers will still respond to `opmnctl` commands, these nodes cannot be used because their node configurations are inactive.

To make a node inactive using the Application Server Control:

1. On the Content DB Home page, stop the node, if it is running.
2. In the Administration section, click **Node Configurations**.
3. Click the name of the node configuration that corresponds to the node you want to make inactive.
4. In the General section, deselect **Active**.
5. Click **OK**.

Although deactivating a node will stop the node, if it is running, it is better to stop the node before you deactivate it.

Managing Services at Run Time

You can use the Application Server Control to create or delete **services** for a particular node. When you create a service, you specify what **service configuration** object provides its properties.

You can make temporary (run-time) changes to a service by modifying the service from the Node page. You can also dynamically configure the Committed Data Cache, Read-only Connection Pool, and the Writeable Connection Pool while the service runs. Changes made to services at run time are lost when the node is restarted.

You can also make permanent changes to a service by modifying its service configuration; see "Managing Service Configurations" on page 8-14 for more information.

This section contains the following topics:

- Creating Services

- Modifying Run-Time Service Parameters
- Managing the Committed Data Cache
- Managing the Connection Pools
- Deleting Services

Creating Services

You can create services for a particular node by modifying the node at run time, or by modifying the appropriate node configuration. You can also create services when you create node configurations.

Creating Services at Run Time

To create a service by modifying the node at run time:

1. On the Content DB Home page, in the Processes section, click the name of the node for which you want to create a service.
2. On the Node page, in the Services section, click **Create**.
3. On the Create Service page, enter a name for the service. It must be unique within the node.
4. Choose a **Service Configuration** on which to base this service.
5. Click **OK** on the Create Service page.

These changes will be lost when the node is restarted.

Permanently Adding Services to a Node

To permanently add a service to a node by modifying its node configuration:

1. On the Content DB Home page, in the Administration section, click **Node Configurations**.
2. Click the name of the node for which you want to add a service.
3. In the Services section, click **Add**.
4. On the Add Service page, enter a name for the service. It must be unique within the node.
5. Select a **Service Configuration** on which to base this service.
6. Select **Active** if you want this service to be automatically started by the node.
7. Click **OK** on the Add Service page.
8. Click **OK** on the Edit Node page.

Changes take effect when the node is restarted.

Modifying Run-Time Service Parameters

You can make run-time changes to services, such as limiting concurrent sessions or choosing whether or not to accept new sessions. Changes you make at run time are lost when the node is restarted. To make permanent changes to a service, edit the service configuration directly. See "Modifying Service Configurations" on page 8-16 for more information.

To modify run-time service parameters:

1. On the Content DB Home page, in the Processes section, click the name of the node that uses the service you want to change.
2. On the Node page, click the name of the service you want to modify.
3. You can change the following properties in the General section:
   - **Concurrent Sessions:** You can have an unlimited number of concurrent sessions, or you can limit concurrent sessions to a specified number. If you have an unlimited number of concurrent sessions, you may run out of memory. See Chapter 2, "Planning for Oracle Content DB Deployment" for more information.
   - **Accepting New Sessions:** Select this option if you want the service to accept additional sessions.
   - **Disposed on Last Disconnected Session:** Select this option if you want the service to shut down automatically when the last session is disconnected.
4. Click **Apply** to save your changes.
5. Use the locator links to return to the Node page.

Changing the Service Configuration Used by the Service

You can change the service configuration for a particular service from the Edit Node Configuration page:

1. On the Content DB Home page, click **Node Configurations**.
2. Click the name of the node configuration that uses the service you want to modify.
3. In the Services section, select the service you want to change and click **Edit**.
4. Select a new service configuration from the **Configuration** list and click **OK**.
5. On the Edit Node page, click **OK**.

Changes take effect when the node is restarted.

Managing the Committed Data Cache

The **Committed Data Cache** provides caching of the attribute values of frequently used objects without a database request, improving performance and scalability. Least recently used data is periodically purged from the cache. Each service has its own Committed Data Cache.

You can make run-time changes to the Committed Data Cache properties for a service using the Application Server Control. You can also view Committed Data Cache statistics for a service. See "Monitoring Service Performance" on page 9-6 for information about viewing or resetting the statistics.

See Chapter 2, "Planning for Oracle Content DB Deployment" for more information about cache settings.

Making Run-Time Changes to Committed Data Cache Properties

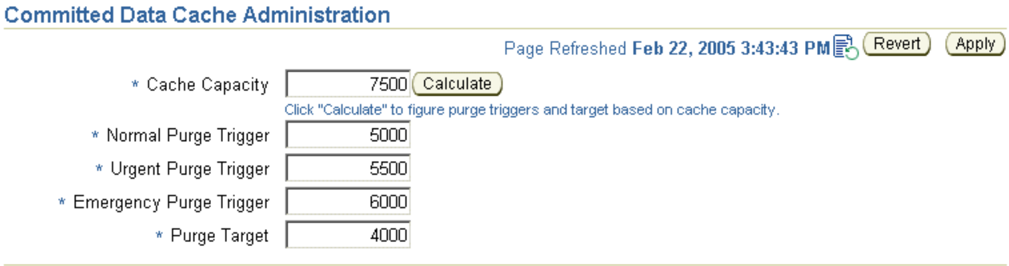
To make run-time changes to Committed Data Cache properties:

1. On the Content DB Home page, click the name of the node that uses the service you want to modify.
2. On the Node page, click the name of the service you want to modify.

3. On the Service page, in the Administration section, click **Committed Data Cache Administration**.

   Figure 7–3 shows the Committed Data Cache Administration page.

Figure 7–3 Committed Data Cache Administration Page



Committed Data Cache Administration

Page Refreshed **Feb 22, 2005 3:43:43 PM**

* Cache Capacity: 7500

Click "Calculate" to figure purge triggers and target based on cache capacity.

* Normal Purge Trigger: 5000

* Urgent Purge Trigger: 5500

* Emergency Purge Trigger: 6000

* Purge Target: 4000

4. You can change the following cache settings:

   - **Cache Capacity:** The absolute maximum size of the data cache of the service, in LibraryObjects. (The LibraryObject class is the base class for all persistent Oracle Content DB objects.) The service data cache holds the attribute values of recently used LibraryObjects.

     After you specify Cache Capacity, you can click **Calculate** to automatically fill in the values for the other parameters based on the capacity you specified.

   - **Normal Purge Trigger:** The cache size, in LibraryObjects, at which the service data cache schedules a low-priority purge of data that has not been recently used.
   - **Urgent Purge Trigger:** The cache size, in LibraryObjects, at which the service data cache schedules a high-priority purge of data that has not been recently used. The value must be greater than the Normal Purge Trigger value.
   - **Emergency Purge Trigger:** The cache size, in LibraryObjects, at which the service data cache performs an immediate purge of data that has not been recently used. The value must be greater than the Urgent Purge Trigger value, but less than the Cache Capacity value.
   - **Purge Target:** The target cache size, in LibraryObjects, upon completion of a purge cycle. The value must be less than the Normal Purge Trigger value.

5. Click **Apply** after you are finished specifying cache settings.

Changes you make at run time are lost when the node is restarted. To make permanent changes to Committed Data Cache properties, edit the service configuration directly. See "Modifying Service Configurations" on page 8-16 for more information.

Table 7–1 maps the properties on the Committed Data Cache Administration page with their service configuration parameter equivalents.

Table 7–1 Committed Data Cache Service Configuration Properties

Property	Service Configuration Parameter Equivalent
Cache Capacity	`IFS.SERVICE.DATACACHE.Size`
Normal Purge Trigger	`IFS.SERVICE.DATACACHE.NormalTrigger`
Urgent Purge Trigger	`IFS.SERVICE.DATACACHE.UrgentTrigger`
Emergency Purge Trigger	`IFS.SERVICE.DATACACHE.EmergencyTrigger`

Table 7–1 (Cont.) Committed Data Cache Service Configuration Properties

Property	Service Configuration Parameter Equivalent
Purge Target	`IFS.SERVICE.DATACACHE.PurgeTarget`

Managing the Connection Pools

There are two connection pools used by each service: the **Read-Only Connection Pool** and the **Writable Connection Pool**. The Read-Only Connection Pool is a set of database connections shared by the sessions to perform database read operations. The Writeable Connection Pool is a set of database connections shared by the sessions to perform database read and write operations within a database transaction.

A minimum number of connections are created in each pool when the service is started. Depending on the number of concurrent operations performed by the sessions, and the type of operations, additional connections may be added to each pool up to a specified maximum.

You can make run-time changes to the Connection Pool properties for a particular service using the Application Server Control. You can also view Read-Only and Writeable Connection Pool statistics for a particular service. See "Monitoring Service Performance" on page 9-6 for information about viewing or resetting the statistics.

See Chapter 2, "Planning for Oracle Content DB Deployment" for more information about connection pool settings.

About the Statement Cache

To improve performance, Oracle Content DB reuses Oracle prepared statements (objects used to query and update the database) when possible. Because Oracle Content DB stores statements in the statement cache, similar queries can reuse existing statements. Least recently used statements are purged when the number of statements in the cache equals the Statement Cache Purge Trigger value.

You can manage statement cache settings from the Connection Pool Administration page. You can also view statement cache statistics (number of attempted purges and purge count) on the Connection Pool Statistics page. See "Monitoring Service Performance" on page 9-6 for more information.

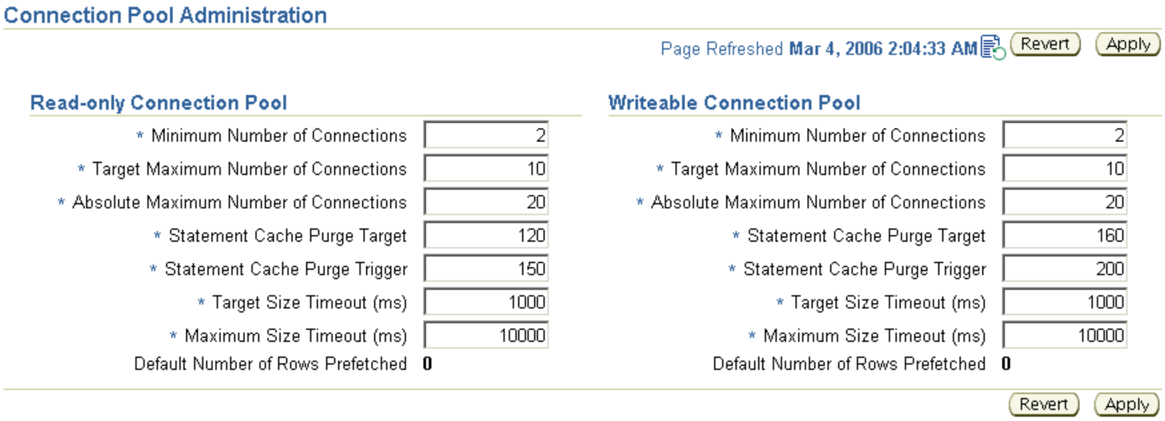
Making Run-Time Changes to Connection Pool Properties

To make run-time changes to Connection Pool properties:

1. On the Content DB Home page, click the name of the node that uses the service you want to modify.
2. On the Node page, click the name of the service you want to modify.
3. On the Service page, in the Administration section, click **Connection Pool Administration**.

   Figure 7–4 shows the Connection Pool Administration page.

Figure 7–4 Connection Pool Administration Page



Connection Pool Administration

Page Refreshed **Mar 4, 2006 2:04:33 AM**

Read-only Connection Pool

* Minimum Number of Connections	2
* Target Maximum Number of Connections	10
* Absolute Maximum Number of Connections	20
* Statement Cache Purge Target	120
* Statement Cache Purge Trigger	150
* Target Size Timeout (ms)	1000
* Maximum Size Timeout (ms)	10000
Default Number of Rows Prefetched	0

Writeable Connection Pool

* Minimum Number of Connections	2
* Target Maximum Number of Connections	10
* Absolute Maximum Number of Connections	20
* Statement Cache Purge Target	160
* Statement Cache Purge Trigger	200
* Target Size Timeout (ms)	1000
* Maximum Size Timeout (ms)	10000
Default Number of Rows Prefetched	0

4. You can change the following properties for each connection pool:

    - **Minimum Number of Connections:** The initial number of database connections in the connection pool.

      If you change this property, ensure the value you specify is greater than the current size for this connection pool. You can view the current connection pool size from the Connection Pool Statistics page. See "Monitoring Service Performance" on page 9-6 for more information.

    - **Target Maximum Number of Connections:** The target maximum number of database connections in the connection pool. The value must be greater than or equal to the Minimum Number of Connections value.

    - **Absolute Maximum Number of Connections:** The absolute maximum number of database connections in the connection pool. The value must be greater than or equal to the Target Maximum Number of Connections value.

    - **Statement Cache Purge Target:** The target cache size, in number of statements, for the statement cache upon completion of a purge cycle. The value must be less than the Statement Cache Purge Trigger value.

    - **Statement Cache Purge Trigger:** The cache size, in number of statements, at which the statement cache schedules a purge.

    - **Target Size Timeout:** The maximum period, in milliseconds, that the service will postpone a connection allocation request when there are no unallocated connections, when the current size of the connection pool is greater than or equal to its target size but less than the maximum size. If a database connection does not become available within this period, a new connection will be created.

    - **Maximum Size Timeout:** The maximum period, in milliseconds, that a service will postpone a connection allocation request when there are no unallocated connections, when the current size of the connection pool is equal to its maximum size. If a database connection does not become available within this period, the allocation request will fail, and an exception will occur.

5. Click **Apply** after you are finished specifying connection pool settings.

Changes you make at run time are lost when the node is restarted. To make permanent changes to Connection Pool properties, edit the service configuration directly. See "Modifying Service Configurations" on page 8-16 for more information.

Table 7–2 maps the properties on the Connection Pool Administration page with their service configuration parameter equivalents.

Table 7–2 Connection Pool Service Configuration Properties

Property	Service Configuration Parameter Equivalent
Minimum Number of Connections	`IFS.SERVICE.CONNECTIONPOOL.READONLY.MinimumSize` `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MinimumSize`
Target Maximum Number of Connections	`IFS.SERVICE.CONNECTIONPOOL.READONLY.TargetSize` `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSize`
Absolute Maximum Number of Connections	`IFS.SERVICE.CONNECTIONPOOL.READONLY.MaximumSize` `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSize`
Statement Cache Purge Target	`IFS.SERVICE.CONNECTIONPOOL.READONLY.StatementCacheTarget` `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheTarget`
Statement Cache Purge Trigger	`IFS.SERVICE.CONNECTIONPOOL.READONLY.StatementCacheSizeTrigger` `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheSizeTrigger`
Target Size Timeout	`IFS.SERVICE.CONNECTIONPOOL.READONLY.TargetSizeTimeout` `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSizeTimeout`
Maximum Size Timeout	`IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSizeTimeout` `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSizeTimeout`

Deleting Services

You can delete services for a node by modifying the node at run time, or by modifying the appropriate node configuration.

If you delete a service with active sessions, and if there are data transfers in progress over those sessions, data may be lost when you delete the service. In addition, any servers using this service will stop accepting new requests.

Deleting Services at Run Time

To delete a service by modifying the node at run time:

1. On the Content DB Home page, in the Processes section, click the name of the node that uses the service you want to delete.
2. On the Node page, in the Services section, select the service you want to delete and click **Delete**. Each node must have one active service.
3. On the Warning page, click **Yes**.

If you delete a service at run time that is defined in the node configuration, the service will reappear on the node when the node is restarted. To permanently delete the service, you must remove it from the node configuration, as described in the following section.

Permanently Removing Services from a Node

To permanently remove a service from a node by modifying its node configuration:

1. On the Content DB Home page, in the Administration section, click **Node Configurations**.
2. Click the name of the node that uses the service you want to remove.
3. In the Services section, select the service you want to remove and click **Remove**.

   You cannot remove a service if it is the only service defined in the node configuration. Each node must have at least one active service.
4. Click **OK**.

Changes take effect when the node is restarted.

Managing Servers at Run Time

You can use the Application Server Control to create or delete **servers** for a particular node. When you create a server, you specify what **server configuration** object provides its properties.

You can make temporary (run-time) changes to a server by modifying the server from the Node page. Changes made to servers at run time are lost when the node is restarted.

You can also make permanent changes to a server by modifying its server configuration. See "Managing Server Configurations" on page 8-17 for more information.

This section contains the following topics:

- Creating Servers
- Starting, Stopping, Restarting, Suspending, and Resuming Servers
- Modifying Run-Time Server Parameters
- Reloading Servers
- Deleting Servers

Creating Servers

You can create servers for a particular node by modifying the node at run time, or by modifying the appropriate node configuration. You can also create servers when you create node configurations.

Creating Servers at Run Time

To create a server by modifying the node at run time:

1. On the Content DB Home page, click the name of the node for which you want to create a server.
2. On the Node page, in the Servers section, click **Create**.
3. On the Create Server page, enter a name for the server. It must be unique within the node.
4. Select a **Service Name** to support this server.
5. Select a **Server Configuration** on which to base this server.

6. Click **OK**.

These changes will be lost when the node is restarted.

Permanently Adding Servers to a Node

To permanently add a server to a node by modifying its node configuration:

1. On the Content DB Home page, in the Administration section, click **Node Configurations**.
2. Click the name of the node for which you want to add a server.
3. In the Servers section, click **Add**.
4. On the Add Server page, enter a name for the server. It must be unique within the node.
5. Select a **Server Configuration** on which to base this service.
6. Select a **Service** to support this server.
7. For **Initial Priority**, select the Java thread priority of the server.
8. Select **Active** to deploy this server on the node at run time. If you do not select this option, this server will not appear in the Servers list on the Node page.
9. Select **Initially Started** if you want this server to be automatically started by the node. You should only select this option for active nodes.
10. Click **OK**.
11. On the Edit Node page, click **OK**.

Changes take effect when the node is restarted.

Starting, Stopping, Restarting, Suspending, and Resuming Servers

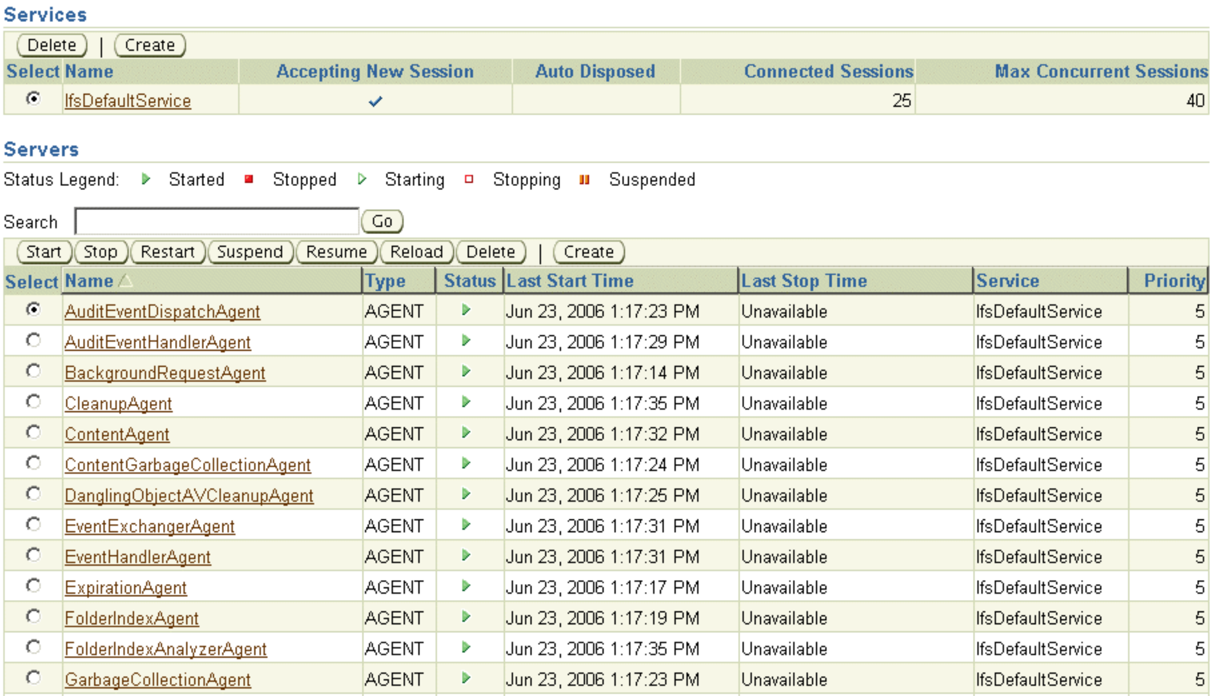
You can manually start, stop, restart, suspend, and resume servers from the Node page. The Create, Delete, and Reload buttons are discussed in separate sections.

To manage servers from the Node page:

1. On the Content DB Home page, click the name of the node that contains the server you want to manage. The Node page appears.

   Figure 7–5 shows the Node page.

Figure 7–5 Services and Servers Section of Node page



Services

Select	Name	Accepting New Session	Auto Disposed	Connected Sessions	Max Concurrent Sessions
●	IfsDefaultService	✓		25	40

Servers

Status Legend: ▶ Started ■ Stopped ▷ Starting □ Stopping ▮▮ Suspended

Select	Name △	Type	Status	Last Start Time	Last Stop Time	Service	Priority
●	AuditEventDispatchAgent	AGENT	▶	Jun 23, 2006 1:17:23 PM	Unavailable	IfsDefaultService	5
○	AuditEventHandlerAgent	AGENT	▶	Jun 23, 2006 1:17:29 PM	Unavailable	IfsDefaultService	5
○	BackgroundRequestAgent	AGENT	▶	Jun 23, 2006 1:17:14 PM	Unavailable	IfsDefaultService	5
○	CleanupAgent	AGENT	▶	Jun 23, 2006 1:17:35 PM	Unavailable	IfsDefaultService	5
○	ContentAgent	AGENT	▶	Jun 23, 2006 1:17:32 PM	Unavailable	IfsDefaultService	5
○	ContentGarbageCollectionAgent	AGENT	▶	Jun 23, 2006 1:17:24 PM	Unavailable	IfsDefaultService	5
○	DanglingObjectAVCleanupAgent	AGENT	▶	Jun 23, 2006 1:17:25 PM	Unavailable	IfsDefaultService	5
○	EventExchangerAgent	AGENT	▶	Jun 23, 2006 1:17:31 PM	Unavailable	IfsDefaultService	5
○	EventHandlerAgent	AGENT	▶	Jun 23, 2006 1:17:31 PM	Unavailable	IfsDefaultService	5
○	ExpirationAgent	AGENT	▶	Jun 23, 2006 1:17:17 PM	Unavailable	IfsDefaultService	5
○	FolderIndexAgent	AGENT	▶	Jun 23, 2006 1:17:19 PM	Unavailable	IfsDefaultService	5
○	FolderIndexAnalyzerAgent	AGENT	▶	Jun 23, 2006 1:17:35 PM	Unavailable	IfsDefaultService	5
○	GarbageCollectionAgent	AGENT	▶	Jun 23, 2006 1:17:23 PM	Unavailable	IfsDefaultService	5

2. On the Node page, in the Servers section, there is a list of all servers for this node. Check the Status column to see whether a particular server is started, stopped, starting, stopping, or suspended. Use the following buttons to manage servers:

   - **Start:** Use this option to start a server that is not running.
   - **Stop:** Use this option to stop a server that is running.
   - **Restart:** Use this option to stop and then start a server that is running. This option does not refresh the server configuration information.
   - **Suspend:** Use this option to suspend a server that is running.
   - **Resume:** Use this option to resume a server that is suspended.

     The Suspend and Resume functions are not available for all protocol servers, including the FTP server.

If a server fails to start, check the node log for errors. For regular nodes, click the **Base Log File** link in the Logging section to view the node log. For HTTP nodes, click **Logs** in the upper right corner of the screen and go to the appropriate log.

Ensuring Servers Are Started When the Node Is Started

Which servers and agents start with the node are defined in the node configuration. Servers and agents marked Active and Initially Started in the node configuration are started automatically when you start the domain.

To ensure that a particular server starts when the node restarts, you must modify the node configuration for the node where the server is running:

1. On the Content DB Home page, in the Administration section, click Node Configurations.
2. Click the name of the node configuration you want to modify.
3. In the Servers section, select the server you want to change and click **Edit**.

4. Select **Initially Started**.
5. Click **OK**.
6. On the Edit Node page, click **OK**.

Modifying Run-Time Server Parameters

You can make run-time changes to servers, such as changing the Java thread priority of the server or changing run-time server properties. Changes you make at run time are lost when the node is restarted or when the server is reloaded. To make permanent changes to a server, edit the server configuration directly. See "Modifying Server Configurations" on page 8-20 for more information.

To modify run-time server parameters:

1. On the Content DB Home page, click the name of the node that contains the server you want to change.
2. On the Node page, click the name of the server you want to modify.
3. In the Priority section, click **Change Priority** to change the Java thread priority of the server. On the Change Priority page, select a new priority and click **OK**. Most servers and agents let you change the Java thread priority at run time, but a few servers, including the FTP server, do not provide this option.
4. The run-time properties for the server are displayed in the Runtime Properties section. Properties that can be modified at run time are displayed as links. Click the name of a property to update it. For example, to allow anonymous connections to the FTP server, click **IFS.SERVER.PROTOCOL.FTP.AnonymousAllowed**, change the **Value** to true, and click **OK**. Some run-time properties can only be modified when the server is stopped.
5. Use the locator links at the top of the page to return to the Node page.

Changing the Server Configuration Used by the Server

To change the configuration used by a server, delete the existing server and then create a new server from the Node page. Alternatively, you can change the configuration for a server from the Edit Node Configuration page:

1. On the Content DB Home page, in the Administration section, click **Node Configurations**.
2. Click the name of the node configuration that contains the server you want to modify.
3. In the Servers section, select the server you want to change and click **Edit**.
4. Select a new server configuration from the **Configuration** drop-down list.
5. Click **OK**.
6. On the Edit Node page, click **OK**.

Changes take effect when the server is reloaded or when the node is restarted.

Reloading Servers

If you modify a server configuration, you need to reload the server before the changes take effect. Restarting a server and reloading a server are different functions:

- **Restart** stops and then starts the server. You can only restart servers that are started. Restarting the server will not pick up changes to server configuration properties.
- **Reload** does the following:
  - Stops the server, if it is not stopped already.
  - Deletes the server.
  - Creates a new instance of the server, picking up any changes to the server configuration properties.
  - Returns the server to the state it was in when you clicked Reload (stopped, running, or suspended).

Both restarting and reloading a server will disconnect any users connected to that server.

To reload a server:

1. On the Content DB Home page, in the Processes section, click the name of the node that contains the server you want to reload.
2. In the Servers section of the Node page, select the server you want to reload (for example, **FtpServer**).
3. Click **Reload**. The server picks up the new server properties.

Deleting Servers

You can delete servers from a node by modifying the node at run time, or by modifying the appropriate node configuration.

Deleting Servers at Run Time

To delete a server by modifying the node at run time:

1. On the Content DB Home page, click the name of the node that contains the server you want to delete.
2. On the Node page, in the Servers section, select the server you want to delete and click **Stop**, if it is not stopped already. You cannot delete a server that is running or suspended.
3. Select the server again and click **Delete**.
4. On the Warning page, click **Yes**. The server still appears in the server list, but the following message is displayed: "This server is configured but not loaded now."

If you delete a server at run time that is defined in the node configuration, the server will reappear on the node when the node is restarted. To permanently delete the server, you must remove it from the node configuration, as described in the following section.

Permanently Removing Servers from a Node

To permanently remove a server from a node by modifying its node configuration:

1. On the Content DB Home page, in the Administration section, click **Node Configurations**.
2. Click the name of the node that contains the server you want to remove.
3. In the Servers section, select the server you want to remove and click **Remove**.

4. Click **OK**.

Changes take effect when the node is restarted.

Managing Oracle Content DB from the Command Line

As an alternative to using the Application Server Control to manage the Oracle Content DB domain and nodes, you can use `opmnctl`, the command-line tool for OPMN. The OPMN command-line tool can be found in:

```
ORACLE_HOME/opmn/bin/
```

Checking Node Status

Use the following command to check the status of Oracle Content DB nodes on the local middle tier:

```
opmnctl status
```

Include the `@farm` option to check nodes on all middle tiers, as follows:

```
opmnctl @farm status
```

Starting, Stopping, or Restarting the Oracle Content DB Domain

Use the following commands to start, stop, or restart Oracle Content DB domain processes across all Oracle Content DB middle tiers:

```
opmnctl @farm startproc ias-component=Content
opmnctl @farm stopproc ias-component=Content
opmnctl @farm restartproc ias-component=Content
```

To start, stop, or restart Oracle Content DB domain processes on the local middle tier, omit the `@farm` option, as follows:

```
opmnctl startproc ias-component=Content
opmnctl stopproc ias-component=Content
opmnctl restartproc ias-component=Content
```

> **Note:** If you have multiple Oracle Content DB domains registered in Oracle Internet Directory, you must specify which domain to start or stop. The first Oracle Content DB domain to be registered is always identified as `Content`, while additional domains are identified as `Content_`*`database_service_name`*. You need to specify the appropriate domain display name in `opmnctl` commands. For example:
>
> ```
> opmnctl @farm startproc ias_component=Content_orcl
> ```
>
> See Appendix A, "Troubleshooting Oracle Content DB" for more information about determining the domain display name.

Starting, Stopping, or Restarting Node Processes

Use the following commands to start, stop, or restart Oracle Content DB nodes (regular and HTTP) on the local middle tier:

```
opmnctl startproc process-type=node_display_name
opmnctl stopproc process-type=node_display_name
opmnctl restartproc process-type=node_display_name
```

For example:

```
opmnctl startproc process-type=OC4J_Content
opmnctl startproc process-type=Node
```

To start, stop, or restart Oracle Content DB processes on a remote middle tier, include the Oracle Application Server instance name for the remote middle tier. For example, use the following command to start a regular node on a remote middle tier:

```
opmnctl @instance:remote_instance_name startproc process-type=Node
```

If you are unsure of which Oracle Application Server instance name to use, use the `opmnctl @farm status` command to list Oracle Application Server instance names.

In rare cases, a regular node will hang and will not respond to `opmnctl` commands. See Appendix A, "Troubleshooting Oracle Content DB" for information about how to solve this problem.

8

Changing Oracle Content DB Configuration Settings

Your initial Oracle Content DB domain configuration is based on default settings. You can change this configuration at any time using the Application Server Control.

When the Oracle Content DB domain is started, it uses the **domain properties** contained in the repository to determine domain behavior, such as the maximum size of a single file that can be uploaded to Oracle Content DB. Each node has a **node configuration** that determines its run-time behavior. Each service has a **service configuration** that determines its size and characteristics. The **server configuration** for each server or agent provides values for properties, such as the default port number or activation period.

This chapter provides information about the following topics:

- Managing Domain Properties
- Managing Node Configurations
- Managing Service Configurations
- Managing Server Configurations

Managing Domain Properties

Domain properties are settings that apply to the entire domain. When the Oracle Content DB domain is started, it uses the domain properties contained in the repository to determine domain behavior, such as the maximum size of a single file that can be uploaded to Oracle Content DB.

You can view all the domain properties using the Application Server Control. Only underlined properties can be changed.

Changing Domain Properties

To change domain properties:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Domain Properties**.
3. On the Domain Properties page, click the name of the property you want to change. Only underlined properties can be changed. See Table 8–1 for a list of properties that can be edited.

   You may need to move to the next page to find some properties, or you can use the **Search** field. For example, enter **workflow** and click **Go** (or press Enter) to see a list of workflow-related domain properties. You can use the question mark (?) and asterisk (*) wildcards.

4. Make the changes to the property and click **OK**.
5. Return to the Content DB Home page and click **Restart Domain**.

Table 8–1 Oracle Content DB Domain Properties That Can Be Edited

Domain Property	Description
`IFS.DOMAIN.ANTIVIRUS.Enabled`	Determines whether Oracle Content DB is configured to work with the Symantec AntiVirus Scan Engine (SAVSE) to provide virus scanning and repair functionality. The default value is false.
`IFS.DOMAIN.ANTIVIRUS.Host`	The host name or IP address of the computer where the SAVSE server is running.
`IFS.DOMAIN.ANTIVIRUS.MaxRepairAttempts`	The number of times the Virus Scan Agent will try to repair a file.
`IFS.DOMAIN.ANTIVIRUS.Port`	The port number for the SAVSE listener.
`IFS.DOMAIN.APPLICATION.ApplicationHost`	The host name of the Oracle Content DB application (where a user connects; for example, `content.oracle.com`).
`IFS.DOMAIN.APPLICATION.ApplicationMountPoint`	The mount point for the Oracle Content DB application (usually `/content/app`). Typically, you do not change this value. If you do change this value, be aware that additional configuration is required.
`IFS.DOMAIN.APPLICATION.ApplicationPort`	The port number for the Oracle Content DB application (typically 7777 on UNIX or 80 on Windows).
`IFS.DOMAIN.APPLICATION.ApplicationUseHttps`	Determines whether the Oracle Content DB application uses SSL. If SSL is enabled, users connect using HTTPS, rather than HTTP (for example, `https://content.oracle.com`).
`IFS.DOMAIN.APPLICATION.RecordApplicationMountPoint`	The mount point for the Oracle Records DB application (usually `/rm/app`). Typically, you do not change this value. If you do change this value, be aware that additional configuration is required.
`IFS.DOMAIN.APPLICATION.WebDavMountPoint`	The mount point for the content/DAV servlet (usually `/content/dav`). Typically, you do not change this value. If you do change this value, be aware that additional configuration is required.
`IFS.DOMAIN.BFILE.AgingEnabled`	Determines whether Oracle Content DB is configured for BFILE aging. The default value is false.
`IFS.DOMAIN.BFILE.ArchivingEnabled`	Determines whether Oracle Content DB is configured for BFILE archiving. The default value is false.
`IFS.DOMAIN.BFILE.Enabled`	If set to true, enables Oracle Content DB to store content as BFILEs. The default value is false.
`IFS.DOMAIN.CREDENTIALMANAGER.AutoUserProvisioningEnabled`	If set to true, enables on-demand enrollment, a process in which Oracle Content DB automatically provisions a new user when the user first signs on.
`IFS.DOMAIN.CREDENTIALMANAGER.ServiceToServiceAuthenticationEnabled`	If set to true, enables Service-to-Service authentication, which allows a trusted partner application to establish user sessions with a digest credential (or basic credential over HTTPS), rather than using individual user credentials.
`IFS.DOMAIN.DOCUMENT.DefinitionObjectExpirationPeriod`	The default time, in seconds, before temporary DefinitionObject instances that were created without specifying an explicit expiration period are freed from the system.

Table 8–1 (Cont.) Oracle Content DB Domain Properties That Can Be Edited

Domain Property	Description
`IFS.DOMAIN.EMAIL.AdministratorAddress`	The e-mail address of an administrator where Site quota warning notifications are sent.
`IFS.DOMAIN.EMAIL.SmtpHost`	The host name for the SMTP server used by Oracle Content DB.
`IFS.DOMAIN.EMAIL.SmtpPort`	The port number for the SMTP server used by Oracle Content DB.
`IFS.DOMAIN.EMAIL.SmtpTimeoutLength`	How long Oracle Content DB waits for the SMTP server to return from sending e-mail.
`IFS.DOMAIN.EMAIL.SmtpUser`	The name of a user for the SMTP server used by Oracle Content DB.
`IFS.DOMAIN.LIBRARYOBJECT.SERVICECONFIGURATION.DefaultServiceConfiguration`	The service configuration used by some internal Oracle Content DB processes to connect to the repository. The default is `SmallServiceConfiguration`.
`IFS.DOMAIN.MEDIA.CONTENTTRANSFER.ContentLimit`	The maximum size of a single file that can be uploaded to Oracle Content DB. The value you specify is interpreted as the maximum number of megabytes or characters allowed for a single upload of data. This limit does not apply to administrators. The value you specify is interpreted in different ways depending on file type: ■ For binary files, this number is the maximum number of megabytes. For example, if you enter 5, the limit will be 5 megabytes for binary files. ■ For text files, such as ASCII or HTML, the number you specify is first converted into bytes, then applied as a maximum character limit, taking into account multibyte encoding. For example, if you enter 5, the limit will be 5 x 1,048,576 (or 5,242,380) characters for text files. Set this property to 0 (the default) if you do not want to limit the size of single-file uploads. Users will then be able to upload any file whose size is within the last calculated available quota, as of the beginning of the upload.
`IFS.DOMAIN.PROTOCOLS.DAV.CleartextAuthenticationEnabled`	Determines whether WebDAV clients can connect to the server using cleartext authentication.
`IFS.DOMAIN.PROTOCOLS.DAV.NullResourceLockExpirationPeriod`	The time period, in seconds, after which namespaces reserved over WebDAV as part of a Null Resource Lock are released. The default value is 3600.
`IFS.DOMAIN.PROTOCOLS.DAV.PersistentCookieName`	The name of the cookie stored by WebDAV clients that use persistent cookies.
`IFS.DOMAIN.PROTOCOLS.DAV.UserAgents`	A custom list of User-Agent headers for well-known WebDAV clients. This property is empty by default; do not provide values unless instructed by Oracle Support Services.
`IFS.DOMAIN.RETENTION.CENTERA.Configuration`	If you have integrated Oracle Content DB with EMC Centera, this property contains the EMC Centera `ADDRESSLIST`, which stores the hostnames or IP addresses of Centera access nodes. On the Edit Property page, you can provide multiple addresses separated by a comma.

Table 8–1 (Cont.) Oracle Content DB Domain Properties That Can Be Edited

Domain Property	Description
`IFS.DOMAIN.RETENTION.SNAPLOCK.Configuration`	If you have integrated Oracle Content DB with Network Appliance SnapLock, this property contains the following settings: - **HOST:** The hostname or IP address of the Network Appliance device - **MOUNTPOINT:** The absolute path where the Network Appliance device is NFS-mounted on the database server - **PORT:** The port used to communicate with the Network Appliance device through HTTP. The default port is 80. - **RELATIVEPATH:** A path relative to the NFS mount point where content will be stored - **SNAPLOCKEXPORTPATH:** The absolute path of the NFS-exported volume
`IFS.DOMAIN.RETENTION.StorageDevice`	The hardware-immutable storage device used for records retention.
`IFS.DOMAIN.RMLIFECYCLEAGENT.EventTarget`	This property is used internally and cannot be changed.
`IFS.DOMAIN.SEARCH.AttemptContextSearchRewrite`	Determines whether Oracle Content DB attempts to generate fast-response SQL for text searches. The default value is true.
`IFS.DOMAIN.WORKFLOW.BPEL.CreationEnabled`	Determines whether Oracle Content DB is configured to integrate with custom BPEL workflows created in Oracle BPEL Process Manager.
`IFS.DOMAIN.WORKFLOW.BPEL.WorklistURL`	The URL of the Oracle BPEL Process Manager Worklist application. You must specify an absolute URL that begins with: `HTTP://`
`IFS.DOMAIN.WS.CleartextAuthenticationRequiresHttps`	If set to true (recommended), does not allow cleartext authentication over Web services, unless the Oracle Content DB application has been configured for SSL.

Managing Node Configurations

The run-time behavior of a node is specified in its **node configuration** object. Each node has its own corresponding node configuration. If you want to make permanent changes to a node, such as changing servers or services, modify the node configuration for the node. If you want to make temporary (run-time) changes to a node, modify the node itself. Changes made at run time are lost when the node is restarted.

You cannot create a node directly using the Application Server Control. Instead, you must first create an active node configuration, and then a corresponding node will be created automatically. Similarly, to delete a node, you must delete its node configuration object (or mark its node configuration as inactive), rather than deleting the node directly.

Nodes and node configurations do not have identical names. HTTP nodes use the name of the corresponding OC4J instance, while regular nodes appear as the display name specified in the node configuration. The display name for each node is the same as the OPMN process type for both regular and HTTP nodes. For example, if you specify Node1 as the display name for a regular node, you can start that node using the following OPMN command:

```
opmnctl startproc process-type=Node1
```

This section describes the following topics:

- Creating Regular Node Configurations
- Creating HTTP Node Configurations
- Modifying Node Configurations
- Deleting Node Configurations
- Configuring Node Loggers

Creating Regular Node Configurations

When you create an active, regular node configuration, a corresponding regular node and its OPMN process type are created automatically.

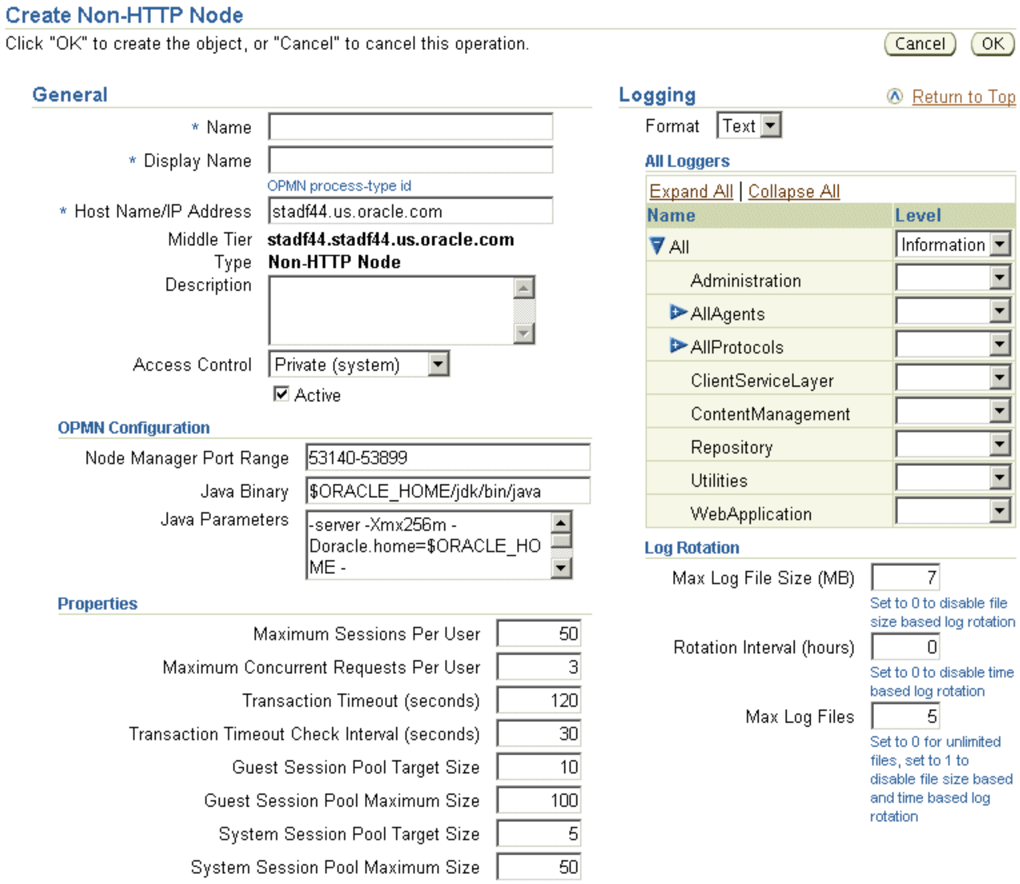
To create a regular node configuration:

1. If you have multiple Oracle Content DB middle tiers, connect to the Application Server Control on the middle tier where you want to add and run the node.
2. On the Content DB Home page, in the Administration section, click **Node Configurations**.
3. On the Node Configurations page, decide whether or not to create a new regular node configuration based on the properties of an existing node configuration.
    - Click **Create Non-HTTP Node** to create the node configuration without basing it on an existing node configuration.
    - Select a regular node configuration and click **Create Like** to base the new node configuration on an existing node configuration.

   In both cases, the New Node Configuration page appears. If you selected **Create Like**, some properties have been filled with those of the existing node configuration.

   Figure 8–1 shows the Create Non-HTTP Node page.

Figure 8–1 Create Non-HTTP Node Page



Create Non-HTTP Node

Click "OK" to create the object, or "Cancel" to cancel this operation.

General

* Name	
* Display Name	
* Host Name/IP Address	stadf44.us.oracle.com
Middle Tier	**stadf44.stadf44.us.oracle.com**
Type	**Non-HTTP Node**
Description	
Access Control	Private (system)

☑ Active

OPMN Configuration

Node Manager Port Range	53140-53899
Java Binary	$ORACLE_HOME/jdk/bin/java
Java Parameters	-server -Xmx256m -Doracle.home=$ORACLE_HOME -

Properties

Maximum Sessions Per User	50
Maximum Concurrent Requests Per User	3
Transaction Timeout (seconds)	120
Transaction Timeout Check Interval (seconds)	30
Guest Session Pool Target Size	10
Guest Session Pool Maximum Size	100
System Session Pool Target Size	5
System Session Pool Maximum Size	50

Logging

Format Text

All Loggers

Name	Level
All	Information
Administration	
AllAgents	
AllProtocols	
ClientServiceLayer	
ContentManagement	
Repository	
Utilities	
WebApplication	

Log Rotation

Max Log File Size (MB)	7
Rotation Interval (hours)	0
Max Log Files	5

Set to 0 to disable file size based log rotation
Set to 0 to disable time based log rotation
Set to 0 for unlimited files, set to 1 to disable file size based and time based log rotation

4. Provide a name for the node configuration. This name must be unique in the domain.

5. Provide additional node configuration properties in the General and Logging sections. See Table 8–2 for detailed information about these properties.

6. If you did not select **Create Like**, click **Add** in the Services section to add a default service for the node. Each node must have at least one active service.

   On the Add Service page, specify:

   - **Name:** Service name.
   - **Configuration:** Which service configuration object provides the configuration properties of the service.
   - **Active:** Whether the service is currently active.

     Inactive services are not automatically started by the node. You must have at least one active service to add servers to this node configuration.

   After you are finished specifying parameters on the Add Service page, click **OK**.

7. If you selected **Create Like**, you may want to edit or remove an existing service.

   - To change service properties, select the service and click **Edit**. On the Edit Service page, change the appropriate information and click **OK**.
   - To remove a service, select it and click **Remove**. Each node must have at least one active service.

8. Click **Add** in the Servers section to choose default servers for the node.

   On the Add Server page, specify:

   - **Name:** Server name.
   - **Configuration:** Which server configuration object provides the configuration parameters of the server. For example, select `FtpServerConfiguration` if you want to run an FTP server on this node.
   - **Service:** Name of the service against which the server will operate.
   - **Initial Priority:** Java thread priority of the server.
   - **Active:** Whether the server is currently active. Inactive servers are not automatically loaded by the node.
   - **Initially Started:** Whether the server is automatically started once loaded.

   After you are finished specifying parameters on the Add Server page, click **OK**.

9. If you selected **Create Like**, you may want to edit or remove an existing server.

   - To change server properties, select the server and click **Edit**. On the Edit Server page, change the appropriate information and click **OK**.

     If you want a particular protocol server to automatically start when the node is started, on the Edit Server page, select **Initially Started**.

   - To remove a server, select it and click **Remove**.

10. Click **OK** on the Create Non-HTTP Node page.

11. Optionally, start the node by selecting it from the Processes list on the Content DB Home page and clicking **Start**.

Creating HTTP Node Configurations

When you create an HTTP node configuration, a corresponding HTTP node and its OC4J instance are deployed automatically. Unlike regular node configurations, you do not specify configuration information when you create HTTP node configurations; the new HTTP node configuration is initially based on default settings. You can edit these default settings later.

To create an HTTP node configuration:

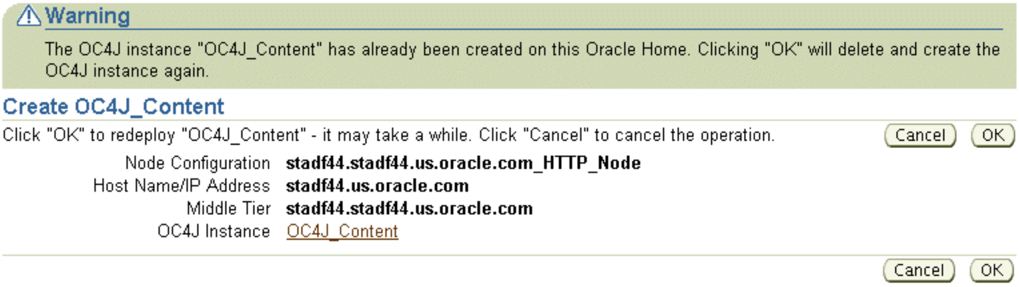
1. If you have multiple Oracle Content DB middle tiers, connect to the Application Server Control on the middle tier where you want to add and run the HTTP node.

2. On the Content DB Home page, in the Administration section, click **Node Configurations**.

3. Click **Create OC4J_Content** to create an HTTP node that supports the Oracle Content DB application. Click **Create OC4J_RM** to create an HTTP node that supports the Oracle Records DB application.

   Figure 8–2 shows the Create OC4J_Content page.

Figure 8–2 Create OC4J_Content Page


Warning

The OC4J instance "OC4J_Content" has already been created on this Oracle Home. Clicking "OK" will delete and create the OC4J instance again.

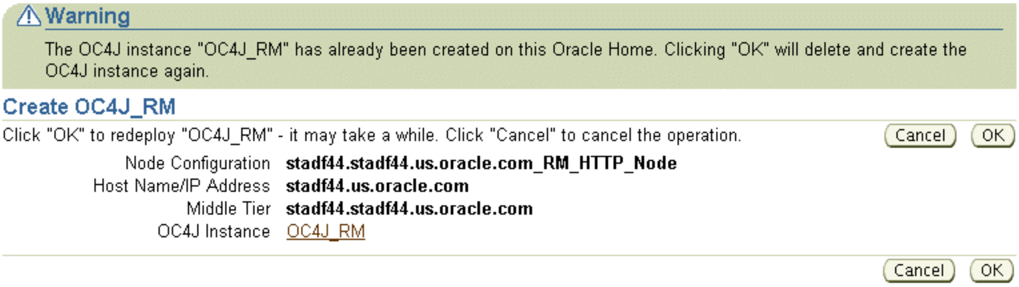
Create OC4J_Content

Click "OK" to redeploy "OC4J_Content" - it may take a while. Click "Cancel" to cancel the operation.

Node Configuration	**stadf44.stadf44.us.oracle.com_HTTP_Node**
Host Name/IP Address	**stadf44.us.oracle.com**
Middle Tier	**stadf44.stadf44.us.oracle.com**
OC4J Instance	OC4J_Content

Figure 8–3 shows the Create OC4J_RM page.

Figure 8–3 Create OC4J_RM Page


Warning

The OC4J instance "OC4J_RM" has already been created on this Oracle Home. Clicking "OK" will delete and create the OC4J instance again.

Create OC4J_RM

Click "OK" to redeploy "OC4J_RM" - it may take a while. Click "Cancel" to cancel the operation.

Node Configuration	**stadf44.stadf44.us.oracle.com_RM_HTTP_Node**
Host Name/IP Address	**stadf44.us.oracle.com**
Middle Tier	**stadf44.stadf44.us.oracle.com**
OC4J Instance	OC4J_RM

4. On the Create OC4J_Content or the Create OC4J_RM page, click **OK**. In rare cases, you may need to provide a name for the node, such as *`middle_tier_name_`*`HTTP_Node` or *`middle_tier_name`*`_RM_HTTP_Node`.
5. Optionally, start the node by selecting it from the Processes list on the Content DB Home page and clicking **Start**.

If you already have HTTP nodes on this middle tier, this operation removes the currently deployed `OC4J_Content` or `OC4J_RM` instance and redeploys the instance again.

Modifying Node Configurations

You can make changes to existing node configurations, such as changing which protocol servers and agents run on a node. Changes take effect when the node is restarted.

To modify a node configuration:

1. On the Content DB Home page, in the Administration section, click **Node Configurations**.
2. On the Node Configurations page, click the name of the node configuration you want to change. You can change both HTTP nodes and regular nodes.
3. Change the node configuration properties, as necessary. The node configuration properties are described in Table 8–2. Some properties apply to regular nodes only.

Table 8–2 Node Configuration Properties

Property Name	Description	Applies to HTTP Node?
Display Name	Appears in the Processes list on the Content DB Home page. This name is also used to identify nodes in `opmnctl` commands.	No. For HTTP nodes, the display name is the same as the OC4J instance for the node (`OC4J_Content` or `OC4J_RM`). You cannot change this value.
Host Name/IP Address	The host name or IP address of the primary network card is displayed by default. If you have multiple network cards, you can change this value to an alternate host name or IP address.	Yes
Description	Description of the node configuration.	Yes
Access Control	The access level associated with the node configuration.	Yes
Active	Whether or not the node configuration is active. Deselect this option to make the node configuration inactive. When you deactivate a node configuration, its corresponding process type is disabled in OPMN. Making a node inactive is an alternative to deleting the node configuration; the configuration information is retained, and you can activate the node later.	Yes
Node Manager Port Range	The port range for the Node Manager process. The default is 53140-53899. You can specify specific ports, a port range, or both. For example, you can specify 53140, 53141, or 53140, 53400-53500. You can enter any valid port number range.	Yes
Java Binary	The Java Binary for the node. The default is *`ORACLE_HOME`*`/jdk/bin/java`.	No
Java Parameters	Edit this value to specify command-line arguments for the Java VM. For example, add `java -Xmx512M` to increase the maximum size of the Java VM memory to 512 MB. To log all garbage collection activity, add `-verbosegc` as an argument.	No. To define Java parameters and arguments for an HTTP node: 1. From the Application Server Home page, click **OC4J_Content**. 2. Click the **Administration** tab, then click **Server Properties**. 3. In the Command Line Options section, update the **Java Options** to include the new -Xmx setting. For example, enter -Xmx430m to specify 430 MB of memory for the Java heap. 4. Click **Apply**. 5. Return to the Application Server Home page and restart **OC4J_Content**.

Table 8–2 (Cont.) Node Configuration Properties

Property Name	Description	Applies to HTTP Node?
Maximum Sessions Per User	The maximum number of user **sessions** allowed for a given user. The default value is 50. If this limit is reached, no new sessions for that user will be allowed on that node until a session ends, either through a logout or a session time out. To allow an unlimited number of sessions for each user, set the value to 0. Because this value is set for each node, different users may experience different session limits. For example, if you have multiple middle tiers, user sessions may be distributed in different ways, depending on load balancing.	Yes
Maximum Concurrent Requests Per User	The maximum number of outstanding requests allowed for a given user. An outstanding request is a request that the server is still processing, such as a search. The default value is 3. To allow an unlimited number of outstanding requests for each user, set the value to 0. Outstanding requests are also limited across all users, through the property `IFS.SERVICE.MaximumConcurrentSessions`. See Appendix D, "Service Configuration Properties" for more information.	Yes
Transaction Timeout (seconds)	The inactivity timeout period for a transaction that spans multiple requests. This setting usually applies to Web services clients, because they are the only clients that can have transactions that span multiple requests. If there is an outstanding transaction and there is no request on the corresponding session for the transaction timeout period, the transaction will time out. The default value is 120. Do not set this property to a value lower than 15.	Yes
Transaction Timeout Check Interval (seconds)	The interval between successive checks for transactions that need to be timed out. The default value is 30. Follow these guidelines for setting this value: ■ This value must be smaller than the Transaction Timeout. ■ Setting a small value for this property may have a performance impact. ■ A large value for this parameter can significantly increase the actual transaction timeout period. For example, if the Transaction Timeout is 120 seconds, and the Transaction Timeout Check Interval is 30 seconds, then a given transaction will time out between 120 and 150 seconds of inactivity, depending on the timing of the transaction check.	Yes

Table 8–2 (Cont.) Node Configuration Properties

Property Name	Description	Applies to HTTP Node?
Guest Session Pool Target Size	The number of sessions kept in the guest session pool. If the number of sessions in the guest pool is equal to the Guest Session Pool Target Size up on the return of a session, the session will be disconnected, rather than returned to the pool. The default value is 10. If you are not allowing guest access, you can set this value to 0.	Yes
Guest Session Pool Maximum Size	The maximum number of guest sessions that can be in use at a given time. The default value is 100. If you are not allowing guest access, you can set this value to 0. This value must be greater than the Guest Session Pool Target Size (if the Guest Session Pool Target Size is greater than 0).	Yes
System Session Pool Target Size	The number of sessions kept in the system session pool. If the number of sessions in the system pool is equal to the System Session Pool Target Size up on the return of a session, the session will be disconnected, rather than returned to the pool. The default value is 5. Do not set this property to a value lower than 5.	Yes
System Session Pool Maximum Size	The maximum number of system sessions that can be in use at a given time. The default value is 50. This value must be greater than the System Session Pool Target Size.	Yes
All Loggers	You can configure the level of logging for this node. See "Configuring Node Loggers" on page 8-12 for more information.	Yes
Format	Whether the log format should be text or XML.	No
Max Log File Size (MB)	The maximum size for the log. The default is 7 MB. Set this value to 0 to disable file size-based log rotation. You should set the Max Log File Size or the Rotation Interval property, or both, to a value other than 0 to keep the log from getting too large.	No
Rotation Interval (hours)	The interval, in hours, that the log is archived and rotated. After this interval, the current log is renamed to include a time stamp, and a new log is created. Set this value to 0 to disable time-based log rotation.	No
Max Log Files	The maximum number of logs allowed. When the maximum number of logs is reached, the oldest log is overwritten. The default value is 5. Set this value to 0 to allow unlimited logs. If you set this value to 1, both file size-based and time-based log rotation are disabled, regardless of the values set for Max Log File Size and Rotation Interval property.	No

4. In the Services section, you can add, edit, or remove services for this node.
   - To add a service, click **Add**, specify information for the service, and click **OK**.

  - To change service properties, select the service and click **Edit**, or click the service name. On the Edit Service page, change the appropriate information and click **OK**.
  - To remove a service, select it and click **Remove**. Each node must have at least one active service.

5. In the Servers section, you can add, edit, and remove protocol servers and agents for this node. You can also activate or deactivate servers for the node.
   - To add a server, click **Add**, specify information for the server, and click **OK**. To actively run a protocol server or agent on this node, make sure to select **Active** and **Initially Started**.
   - To change server properties, select the server and click **Edit**, or click the server name. On the Edit Server page, change the appropriate information and click **OK**.

     If you want a server to automatically start when the node is started, on the Edit Server page, select **Active** and **Initially Started**.
   - To remove a server, select it and click **Remove**.
   - To activate or deactivate multiple servers, click **Activate/Deactivate**. On the Activate/Deactivate Servers page, you can move servers between the Active Servers list and the Inactive Servers list. Then, click **OK**.
6. On the Edit Node page, click **OK** to save the changes. You must restart the node for your changes to take effect.

Deleting Node Configurations

Deleting a node configuration also deletes the node process that is based on that node configuration. Typically, you only delete node configurations that are local to the current middle tier. In rare cases, however, such as when a middle tier fails, you may need to delete a node configuration on a remote middle tier.

To delete a node configuration:

1. On the Content DB Home page, stop the node, if it is running.
2. In the Administration section, click **Node Configurations**.
3. On the Node Configurations page, select the node configuration you want to delete.
4. Click **Delete**. If you to delete an HTTP node, its corresponding OC4J instance is also deleted.
5. On the Warning page, click **Yes**. The node configuration is deleted.

Deactivating Nodes

Making a node inactive is an alternative to deleting the node configuration. An inactive node is removed from the domain and is disabled in OPMN, but the configuration information is kept so that you can activate the node later. See "Deactivating Nodes" on page 7-5 for more information.

Configuring Node Loggers

You can configure **loggers** for each node to fine-tune the level of information you want to collect in each node log. For example, you can specify a more detailed level of logging for a particular protocol server or agent. All messages are logged in English.

You can configure loggers from the Node page, or you can configure loggers by modifying the node configuration for a node.

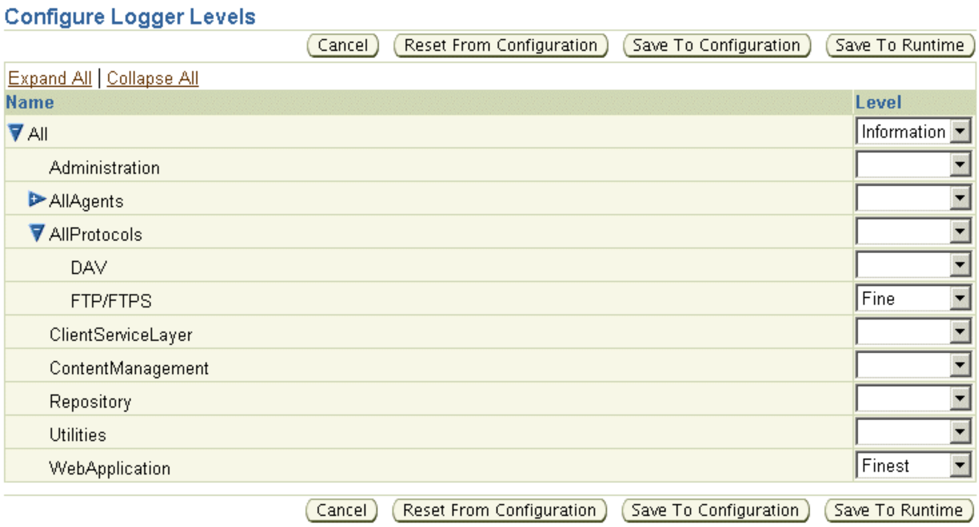
Configuring Loggers from the Node Page

To configure loggers from the Node page:

1. On the Content DB Home page, in the Processes section, click the name of the node for which you want to configure loggers.
2. From the Node page, in the Loggers section, you can see a list of loggers and their current log level by expanding the **All Loggers** heading.
3. Click **Configure Loggers** to change log levels for particular loggers.

   Figure 8–4 shows the Configure Logger Levels page.

Figure 8–4 Configure Logger Levels Page



Name	Level
All	Information
Administration	
AllAgents	
AllProtocols	
DAV	
FTP/FTPS	Fine
ClientServiceLayer	
ContentManagement	
Repository	
Utilities	
WebApplication	Finest

4. On the Configure Logger Level page, specify logging levels for loggers you want to configure. For example, you can increase the log level for FTP (under the AllProtocols heading) to get more detailed logging on the Oracle Content DB FTP server. The available log levels are:
   - **Severe:** Log only nonrecoverable problems
   - **Warning:** Log only recoverable problems
   - **Important:** Log messages that are deemed important
   - **Information:** General level of log information
   - **Fine:** Level for debugging or tracing key operations
   - **Finer:** Level for debugging or tracing the entry and exit of methods
   - **Finest:** Level for debugging or tracing within a method
5. Click **Save To Runtime** if you want your changes to take effect for the current node, but you do not want your changes to be saved when the node is restarted.
6. Click **Save To Configuration** if you want your changes to become a permanent part of the node configuration. Your changes will be retained when the node is restarted.

7. Click **Reset From Configuration** to remove any changes you made to this node at run time, and to reset the values based on the values in the node configuration.

Configuring Loggers by Modifying the Node Configuration

To configure loggers by modifying the node configuration for a particular node:

1. On the Content DB Home page, in the Administration section, click **Node Configurations**.
2. On the Node Configurations page, click the name of the node configuration for which you want to configure loggers.
3. In the All Loggers section, specify logging levels for loggers you want to configure. For example, you can increase the log level for FTP (under the AllProtocols heading) to obtain more detailed logging on the Oracle Content DB FTP server. The available log levels are:
   - **Severe:** Log only nonrecoverable problems
   - **Warning:** Log only recoverable problems
   - **Important:** Log messages that are deemed important
   - **Information:** General level of log information
   - **Fine:** Level for debugging or tracing key operations
   - **Finer:** Level for debugging or tracing the entry and exit of methods
   - **Finest:** Level for debugging or tracing within a method
4. Click **OK** to save the changes.

Restart the node based on this node configuration for your changes to take effect.

Managing Service Configurations

A **service configuration** holds the default values used when a service is started for an Oracle Content DB node. This section explains how to manage service configurations using the Application Server Control.

This section contains the following topics:

- About Service Configurations
- Creating Service Configurations
- Modifying Service Configurations
- Deleting Service Configurations

About Service Configurations

Each service configuration specifies values for service properties such as credential manager settings, the sizes of the cache and database connection pools, and the maximum number of sessions. See Appendix D, "Service Configuration Properties" for a complete list of service configuration parameters. Service configurations are uniquely named in a domain.

Whenever a new Oracle Content DB schema is created, three service configuration objects are generated:

- `SmallServiceConfiguration`

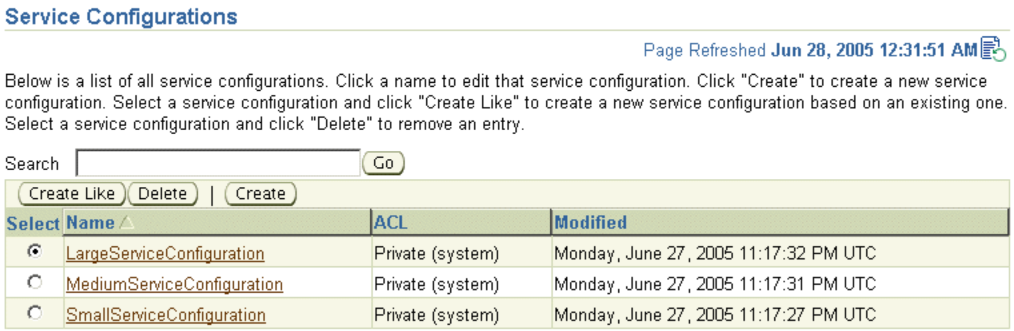
- `MediumServiceConfiguration`
- `LargeServiceConfiguration`

These objects are named to reflect the sizes of their data caches.

Use the Application Server Control to create or edit service configuration objects. The services read their service configuration properties only when they start. You must stop and restart the affected nodes for changes to take effect. The changes you make this way are applied each time you start a service and overwrite any changes you make on a service while it is running.

Figure 8–5 shows the Service Configurations page.

Figure 8–5 Service Configurations Page



Service Configurations

Page Refreshed **Jun 28, 2005 12:31:51 AM**

Below is a list of all service configurations. Click a name to edit that service configuration. Click "Create" to create a new service configuration. Select a service configuration and click "Delete" to remove an entry. Select a service configuration and click "Create Like" to create a new service configuration based on an existing one.

Select	Name	ACL	Modified
●	LargeServiceConfiguration	Private (system)	Monday, June 27, 2005 11:17:32 PM UTC
○	MediumServiceConfiguration	Private (system)	Monday, June 27, 2005 11:17:31 PM UTC
○	SmallServiceConfiguration	Private (system)	Monday, June 27, 2005 11:17:27 PM UTC

Similar to node configuration properties, you can change run-time service properties, change to a different service configuration, alter service configuration properties permanently, or create a new service configuration.

Creating Service Configurations

Use the Application Server Control to create service configurations.

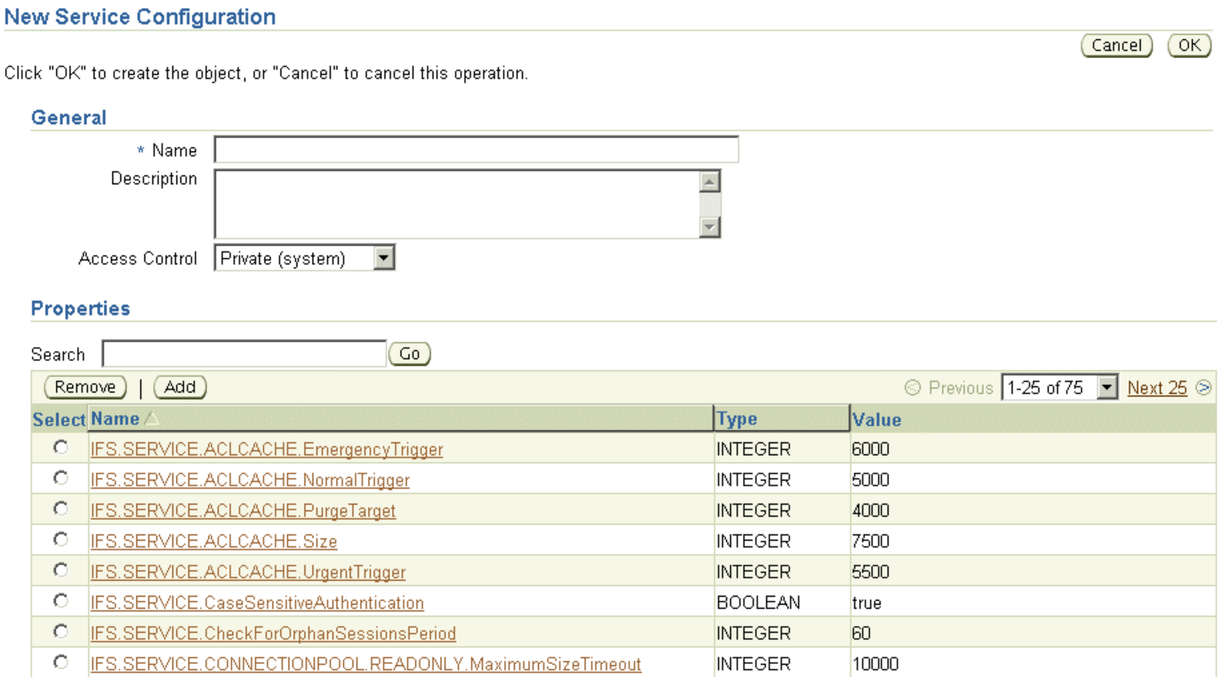
To create a new service configuration:

1. On the Content DB Home page, in the Administration section, click **Service Configurations**.
2. On the Service Configurations page, decide whether or not to create a new service configuration based on the properties of an existing service configuration.
    - Select a service configuration and click **Create Like** to base the new service configuration on an existing service configuration (highly recommended).
    - Click **Create** to create the service configuration without basing it on an existing configuration.

    In both cases, the New Service Configuration page appears. If you clicked **Create Like**, the service configuration properties have been filled with those of the existing service.

    Figure 8–6 shows the New Service Configuration page.

Figure 8–6 New Service Configuration Page



Click "OK" to create the object, or "Cancel" to cancel this operation.

* Name

Description

Access Control: Private (system)

Select	Name	Type	Value
○	IFS.SERVICE.ACLCACHE.EmergencyTrigger	INTEGER	6000
○	IFS.SERVICE.ACLCACHE.NormalTrigger	INTEGER	5000
○	IFS.SERVICE.ACLCACHE.PurgeTarget	INTEGER	4000
○	IFS.SERVICE.ACLCACHE.Size	INTEGER	7500
○	IFS.SERVICE.ACLCACHE.UrgentTrigger	INTEGER	5500
○	IFS.SERVICE.CaseSensitiveAuthentication	BOOLEAN	true
○	IFS.SERVICE.CheckForOrphanSessionsPeriod	INTEGER	60
○	IFS.SERVICE.CONNECTIONPOOL.READONLY.MaximumSizeTimeout	INTEGER	10000

3. In the General section, enter a name for the new service configuration.
4. Enter a description of the service.
5. Assign an access level to the configuration by selecting from the **Access Control** list.
6. Add, remove, or update the properties of the new service.
7. Click **OK**.

Modifying Service Configurations

You can use the Application Server Control to make changes to service configurations, such as changing the capacity of the Committed Data Cache or changing the number of maximum concurrent sessions.

To modify a service configuration:

1. On the Content DB Home page, in the Administration section, click **Service Configurations**.
2. On the Service Configurations page, click the name of the service configuration you want to change.
3. On the Edit page, update the information in the General section, as necessary:
   - **Description:** Enter a description of the service configuration.
   - **Access Control:** Keep the default value.
4. To add new properties for this service configuration, follow these steps:
   a. In the Properties section, click **Add**.
   b. Provide a name for the new property.

   c. Select a **Type** (such as string, integer, or Boolean). The page refreshes to display the appropriate **Value** field. For example, if you select BOOLEAN, a true or false list is displayed.
   d. Enter or select a value for the property.
   e. Click **OK**.
5. To edit a service configuration property, click the name of the property, update the value, and click **OK**.
6. To remove a property from this service configuration, select the property, click **Remove**, then click **Yes**.
7. Click **OK**.

Services only read their service configuration properties as they start. You must stop and restart the node on which the service is running before your changes will take effect. When the node restarts, the changes you made to the service configuration overwrite any run-time changes made on the service.

Deleting Service Configurations

You cannot delete a service configuration that is being used by an active service. If the service configuration you want to delete is being used by an active service, perform one of the following tasks:

- Change the service configuration being used by the service by modifying the node configuration
- Delete the service from the node configuration

You cannot delete the service if it is the only service defined in the node configuration. Each node must have at least one active service.

To delete a service configuration:

1. On the Content DB Home page, in the Administration section, click **Service Configurations**.
2. On the Service Configurations page, select the service configuration you want to delete.
3. Click **Delete**.
4. Click **Yes** to confirm that you want to delete the service configuration.

Managing Server Configurations

A **server configuration** holds the default values used when a server is started for an Oracle Content DB node. This section explains how to manage service configurations using the Application Server Control.

This section contains the following topics:

- About Server Configurations
- Creating Server Configurations
- Modifying Server Configurations
- Deleting Server Configurations

About Server Configurations

Server configurations specify their server types as Java classnames. In addition to the server type, each server configuration specifies values for parameters relevant to that type. See Appendix E, "Server Configuration Properties" for more information. For example, a server configuration for the Oracle Content DB FTP server specifies the FTP port number, whether anonymous FTP connections are allowed, and the connection timeout period.

Most of the server configuration information is used by the server itself. Only the server Java class entry is used by the node to instantiate a new server.

When Oracle Content DB is installed, server configurations are automatically created for each protocol server and agent. You can edit these configurations, or create additional server configurations using the Application Server Control. Any changes you make will appear the next time the node is restarted, or when the server is unloaded and then loaded again.

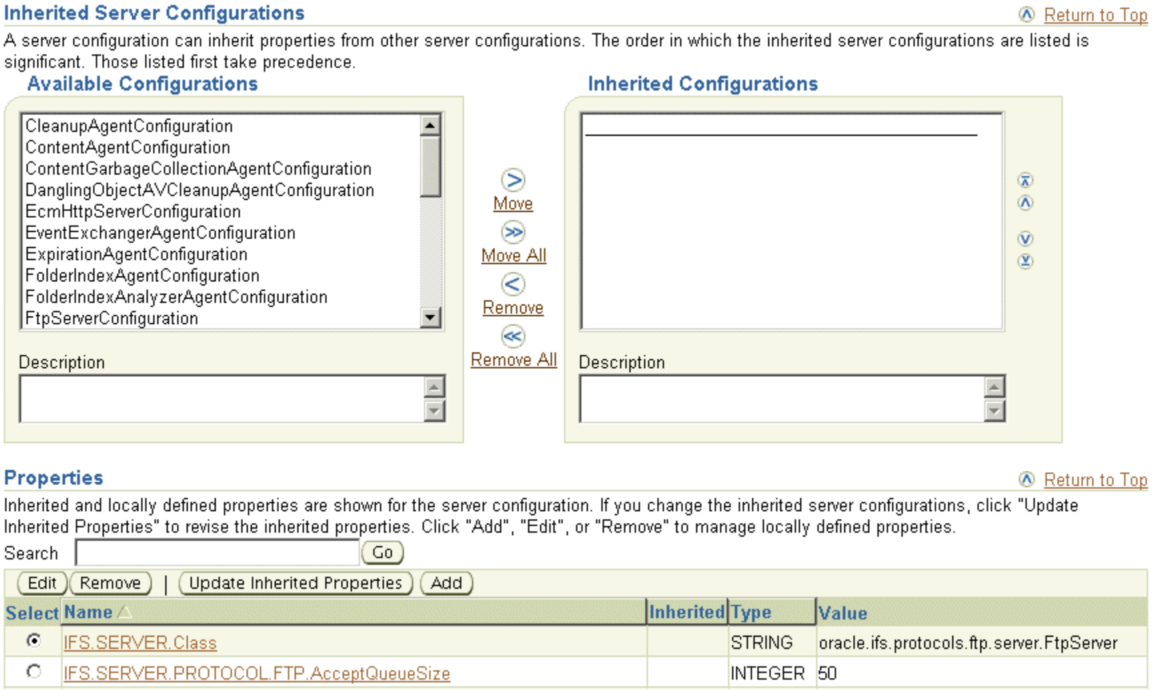
Server configuration objects are of two types:

- **Abstract:** Used to set base values for the properties, which can then be inherited by some other configuration. You cannot start a server from an abstract server configuration.
- **Non-abstract:** Can be used to start servers.

When you create a new server configuration, you can let it inherit the properties from one or more server configurations. You can use the same values as inherited, or use different values.

Inheritance operations are accessed from the New Server Configuration page, shown in Figure 8–7. See "Creating Server Configurations" on page 8-19 for more information on creating new server configurations.

Figure 8–7 Inheritance Operations on the New Server Configuration Page



Inherited Server Configurations
Return to Top
Available Configurations
Inherited Configurations
CleanupAgentConfiguration
ContentAgentConfiguration
ContentGarbageCollectionAgentConfiguration
DanglingObjectAVCleanupAgentConfiguration
EcmHttpServerConfiguration
EventExchangerAgentConfiguration
ExpirationAgentConfiguration
FolderIndexAgentConfiguration
FolderIndexAnalyzerAgentConfiguration
FtpServerConfiguration
Move
Move All
Remove
Remove All
Description
Description
Properties
Return to Top
Search
Go
Edit
Remove
Update Inherited Properties
Add

A server configuration can inherit properties from other server configurations. The order in which the inherited server configurations are listed is significant. Those listed first take precedence.

Inherited and locally defined properties are shown for the server configuration. If you change the inherited server configurations, click "Update Inherited Properties" to revise the inherited properties. Click "Add", "Edit", or "Remove" to manage locally defined properties.

Select	Name	Inherited	Type	Value
●	IFS.SERVER.Class		STRING	oracle.ifs.protocols.ftp.server.FtpServer
○	IFS.SERVER.PROTOCOL.FTP.AcceptQueueSize		INTEGER	50

Changing Values of Inherited Properties

To change the value of an inherited property, create a new property in the inherited server configuration that is identical in name to the one in the parent server configuration, but has values that override those in the parent server configuration.

Viewing Inherited Properties

View the inherited properties to determine whether the property in the current server configuration object is local to this object or taken from a parent server configuration object. You can also differentiate between inherited server configuration objects and those that are local to the server configuration.

Creating Server Configurations

Use the Application Server Control to create new server configurations.

To create a new server configuration:

1. On the Content DB Home page, in the Administration section, click **Server Configurations**.
2. On the Server Configurations page, decide whether or not to create a new server configuration based on the properties of an existing server.
    - Select a server configuration and click **Create Like** to base the new server configuration on an existing configuration.
    - Click **Create** to create the server configuration without basing it on an existing configuration.

    In both cases, the New Server Configuration page appears. If you clicked **Create Like**, the server configuration properties have been filled with those of the existing server.
3. On the New Server Configuration page, in the General section, enter a name for the new server configuration.
4. Enter a description of the server.
5. Keep the default value for **Access Control**.
6. Select **Abstract** to prevent this server from being instantiated. An abstract server configuration is used to set base values for properties, which can then be inherited by another server configuration. You cannot start a server from an abstract server configuration.
7. In the Inherited Server Configurations section, select the existing configurations from which the new configuration will inherit properties. Select configurations from the **Available Configurations** list and move them to the **Selected Configurations** list.
8. If you change the list of inherited server configurations, click **Update Inherited Properties** in the Properties section to display the properties of the inherited server configurations.

    The order of the items in the Inherited Configurations list determines which configuration takes precedence.
9. To edit server configuration properties, follow these steps:
    a. In the Properties section, select the property you want to change and click **Edit**.

   b. Update the value of the property.
   c. Click **OK**.

   For example, to change the FTP port number for a server configuration based on the FtpServerConfiguration, click **IFS.SERVER.PROTOCOL.FTP.Port**, update the value, and click **OK**.

   Inherited server configuration properties cannot be edited. Inherited properties display an icon in the Inherited column, and their names are not rendered as links. To change the value of these properties, add a new property that is identical in name to the inherited property, but with a value that overrides the value of the inherited property.

10. To add new server configuration properties, follow these steps:
    a. Click **Add** in the Properties section.
    b. Enter a name for the new property. If you are adding a property to override an inherited property, make sure the name matches the inherited property.
    c. Select a **Type** (such as string, integer, or Boolean). The page refreshes to display the appropriate **Value** field. For example, if you select **BOOLEAN**, a true or false list is displayed.
    d. Enter or select a value for the property.
    e. Click **OK**. If you added a property to override an inherited property, the property name changes to a link, and the Inherited icon no longer appears.
11. To remove server configuration properties, select a property and click **Remove**.
12. After you complete the server configuration, click **OK**.

Modifying Server Configurations

You can use the Application Server Control to make changes to server configurations, such as changing which configurations to inherit and editing, adding, or removing server configuration properties. See Appendix E, "Server Configuration Properties" for more information about specific server configuration parameters.

To modify an existing server configuration:

1. On the Content DB Home page, in the Administration section, click **Server Configurations**.
2. On the Server Configurations page, click the name of the server configuration you want to modify.
3. On the Edit page, update the information in the General section as necessary:
   - **Description:** Enter a description of the server configuration.
   - **Access Control:** Keep the default value.
   - **Abstract:** Choose whether to make the server configuration abstract. An abstract server configuration is used to set base values for properties, which can then be inherited by some other server configuration. You cannot start a server from an abstract server configuration.
4. In the Inherited Server Configurations section, use the arrow buttons to add or remove server configurations from which this server configuration will inherit properties.

5. If you change the list of inherited server configurations, click **Update Inherited Properties** in the Properties section to display the properties of the inherited server configurations.

   The order of the items in the Inherited Configurations list determines which configuration takes precedence.

6. To edit server configuration properties, follow these steps:
   a. In the Properties section, select the property you want to change and click **Edit**.
   b. Update the value of the property.
   c. Click **OK**.

      For example, to change the FTP port number for a server configuration based on the FtpServerConfiguration, click **IFS.SERVER.PROTOCOL.FTP.Port**, update the value, and click **OK**.

      Inherited server configuration properties cannot be edited. Inherited properties display an icon in the Inherited column, and their names are not rendered as links. To change the value of these properties, add a new property that is identical in name to the inherited property, but with a value that overrides the value of the inherited property.

7. To add new server configuration properties, follow these steps:
   a. Click **Add** in the Properties section.
   b. Enter a name for the new property. If you are adding a property to override an inherited property, make sure the name matches the inherited property.
   c. Select a **Type** (such as string, integer, or Boolean). The page refreshes to display the appropriate **Value** field. For example, if you select BOOLEAN, a true or false list is displayed.
   d. Enter or select a value for the property.
   e. Click **OK**. If you added a property to override an inherited property, the property name changes to a link, and the Inherited icon no longer appears.

8. To remove server configuration properties, select a property and click **Remove**.
9. After you complete the server configuration, click **OK**.

Servers only read their server configuration properties when they are reloaded, or when the node is restarted. You must reload the server before your changes will take effect. See "Reloading Servers" on page 7-15 for more information. These server configuration changes overwrite changes you make on a server while it is running.

Deleting Server Configurations

You cannot delete a server configuration that is being used by an active server. If the server configuration you want to delete is being used by an active server, first edit the node configuration to remove the server, then delete the server configuration. Alternatively, you can change the server configuration being used by the server.

To delete a server configuration:

1. On the Content DB Home page, in the Administration section, click **Server Configurations**.
2. On the Server Configurations page, select the server configuration you want to delete.

3. Click **Delete**.
4. On the Warning page, click **Yes**.

9

Monitoring Domain, Node, Service, and Server Performance

Use the Application Server Control to monitor Oracle Content DB domain, node, service, and server performance. You can use this information to get an overall picture of the performance of the domain, or to determine whether the configuration of the domain needs to be changed.

This chapter provides information about the following topics:

- Monitoring Domain Performance
- Monitoring Node Performance
- Monitoring Service Performance
- Monitoring Server Performance
- Viewing Logs
- Accessing Metrics and Monitoring Metric Alerts

Monitoring Domain Performance

You can use the Application Server Control to view different types of performance information for the Oracle Content DB domain. This section contains the following topics:

- About Oracle Content DB Performance Metrics
- Viewing Performance Information
- Configuring Performance Metrics

About Oracle Content DB Performance Metrics

There are three types of Oracle Content DB performance metrics: repository metrics, Dynamic Monitoring Service (DMS) metrics, and other metrics. See "Monitoring Server Performance" on page 9-7 for information about DMS metrics.

Repository metrics are metrics that apply to the entire Oracle Content DB domain. These metrics include:

- Domain Response
- Documents
- Documents By MIME Type
- Users

- Users By Site
- Libraries By Site
- Nodes
- Sessions By Server (Node)
- Sessions By Server (Domain)
- All Sessions

Other Oracle Content DB performance metrics include:

- Response
- Resource Usage
- Processes
- Web Application URL Timing
- Records DB Application URL Timing
- Load Balanced Web Application URL Timing
- Load Balanced Records DB Application URL Timing

Some metrics must be configured for particular middle tiers. See "Configuring Performance Metrics" on page 9-4 for more information.

Viewing Performance Information

You can view Oracle Content DB performance metrics in two ways:

- All Oracle Content DB metrics can be viewed from the All Metrics pages, as long as they are being collected on that middle tier.
- Repository metrics can also be viewed from the Domain Performance & Statistics pages, which provide information in a more graphical format than the All Metrics pages. These pages are not available on middle tiers where repository metrics are not being collected.

Using the All Metrics Link

All Oracle Content DB performance metrics that are being collected on a middle tier can be accessed from the All Metrics pages in the Application Server Control. To access these pages, from the Performance section of the Content DB Home page, click **All Metrics**.

To view information about a particular metric, click the metric name, then click **Help** on the resulting Metric Detail page.

Using the Domain Performance & Statistics Pages

The Domain Performance & Statistics pages in the Application Server Control provide tables and charts that present information about Oracle Content DB users, Libraries, documents, sessions, and overall usage patterns. This information can help you evaluate system performance and guide you in making changes to your configuration.

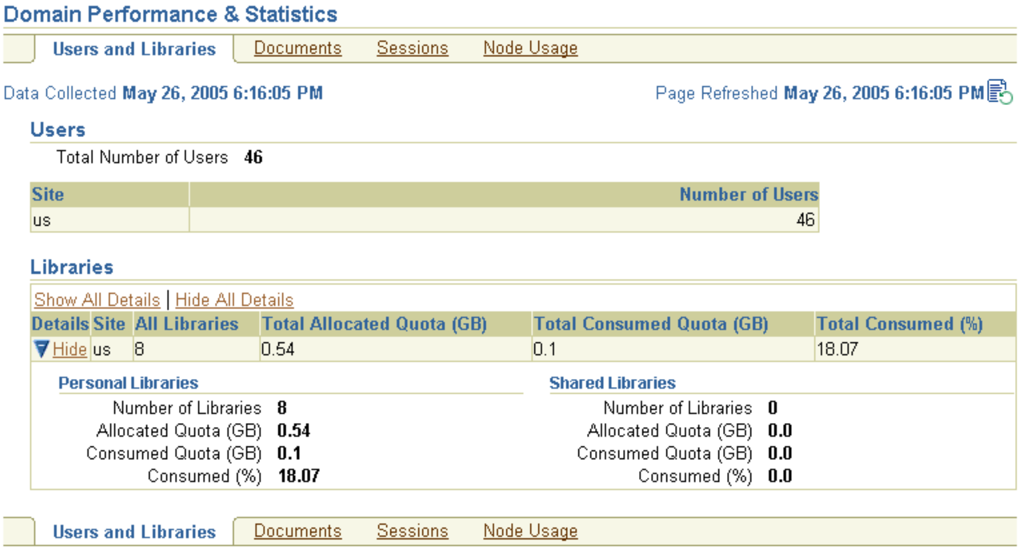
The Domain Performance & Statistics pages are only available on middle tiers that have been configured for repository metrics. See "Configuring Performance Metrics" on page 9-4 for more information.

To view domain performance information:

1. On the Content DB Home page, click **Domain Performance & Statistics**.

   Figure 9–1 shows the Domain Performance & Statistics page.

Figure 9–1 Domain Performance & Statistics Page



Domain Performance & Statistics

Data Collected **May 26, 2005 6:16:05 PM**

Page Refreshed **May 26, 2005 6:16:05 PM**

Users

Total Number of Users **46**

Site	Number of Users
us	46

Libraries

Show All Details | Hide All Details

Details	Site	All Libraries	Total Allocated Quota (GB)	Total Consumed Quota (GB)	Total Consumed (%)
▼ Hide	us	8	0.54	0.1	18.07

Personal Libraries

Number of Libraries **8**
Allocated Quota (GB) **0.54**
Consumed Quota (GB) **0.1**
Consumed (%) **18.07**

Shared Libraries

Number of Libraries **0**
Allocated Quota (GB) **0.0**
Consumed Quota (GB) **0.0**
Consumed (%) **0.0**

2. Select one of the four subtabs:

   - The **Users and Libraries** subtab provides information about the total number of users and the number of users for each Site, and provides information about Personal and Shared Libraries for each Site.
   - The **Documents** subtab provides systemwide information about documents.
   - The **Sessions** subtab lets you view the connected sessions by server type.
   - The **Node Usage** subtab lets you monitor sessions, threads, and memory by node and host.

3. To refresh the information for the **Sessions** or **Node Usage** subtabs, refresh your browser, or click the Refresh Data icon in the upper right portion of the page.

   Because data for the **Users and Libraries** and **Documents** subtabs is only collected at preset intervals, refreshing the page will not cause the data to be collected again. To see the last time the data was collected on these tabs, look at the Data Collection Time displayed in the upper left corner of the page.

4. To move between the table view and the chart view, make a selection from the **Select a View** list.

Table 9–1 lists the various charts, graphs, and tables, and shows you which subtab and view names you need to select to access the information.

Table 9–1 Reference to Statistical Information About the Domain and Nodes

Chart, Graph, or Table Name	Statistics or Information Displayed	Subtab	Select a View Item
Users	■ Total Number of Users ■ Total Number of Users by Site	Users and Libraries	Not applicable
Libraries	Tabular display showing: ■ Total number of Libraries for each Site ■ Total allocated quota for each Site ■ Total consumed quota for each Site ■ Percentage of quota consumed for each Site These statistics are also available for Personal and Shared Libraries for each Site; click **Show** in the Details column to access this information.	Users and Libraries	Not applicable
Document Table	Document distribution and space consumption by MIME type.	Documents	Table
Document Distribution Chart	Space consumed, displayed by MIME type (displays a bar chart comparing quantities of the different types of documents stored in the system).	Documents	Distribution Chart
Document Consumption Chart	Space consumed, displayed by MIME type.	Documents	Consumption Chart
Sessions Table	Tabular display of the total number of connected sessions for each protocol server or agent.	Sessions	Table
Sessions Chart	Pie chart of total number of connected sessions for each protocol server or agent. The sessions for all the agents are displayed as a combined result.	Sessions	Chart
Node Usage Table	Tabular display of node name, host name and IP address, number of sessions, number of threads, and JVM total/free/used memory for each node.	Node Usage	Table
Node Usage Chart	Bar charts showing the same information as the Overall Usage Table.	Node Usage	Chart

Configuring Performance Metrics

You can use the Application Server Control to select which Oracle Content DB performance metrics to configure on the current middle tier. For example, you can collect metrics related to Oracle Content DB Web application response time.

To configure performance metrics:

1. On the Content DB Home page, in the Performance section, click **Metric Configuration**.
2. You can collect repository metrics on this middle tier. To do this, select **Run Repository Metric?**, and provide the Oracle Content DB schema password and the database connect descriptor. If you do not know the database connect descriptor, you can copy it from the Content DB Home page.

To avoid the potential performance impact of duplicate metric collection, only run repository metrics on one middle tier. Be aware that the Domain Performance & Statistics pages are only available from middle tiers on which repository metrics are collected.

3. You can collect metrics related to Oracle Content DB Web application response time on this middle tier.
    - To collect metrics related to the Oracle Content DB Web application URL for this middle tier, select **Run Web Application Response Time Metric?**, and provide the correct Oracle Content DB Web application URL for this middle tier.
    - To collect metrics related to the load-balanced URL for the Oracle Content DB Web application, select **Run Load Balanced Web Application Response Time Metric?**, and provide the correct Oracle Content DB load-balanced Web application URL.
4. You can collect metrics related to Oracle Records DB Web application response time on this middle tier.
    - To collect metrics related to the Oracle Records DB Web application URL for this middle tier, select **Run Records DB Application Response Time Metric?**, and provide the correct Oracle Records DB Web application URL for this middle tier.
    - To collect metrics related to the load-balanced URL for the Oracle Records DB Web application, select **Run Load Balanced Records DB Application Response Time Metric?**, and provide the correct Oracle Records DB load-balanced Web application URL.

    If Oracle Records DB was not enabled, these metrics will report that the Oracle Records DB Web application URLs are not available.
5. Click **OK**.

Monitoring Node Performance

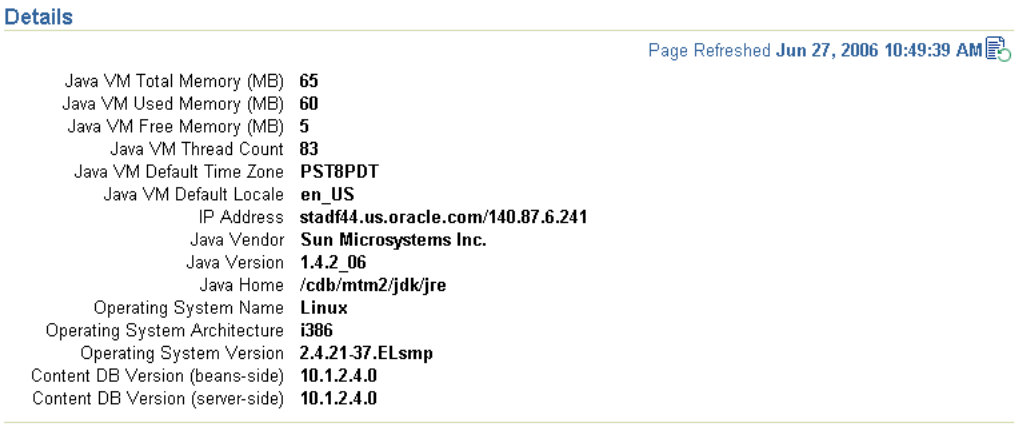
You can use the Application Server Control to view performance information about both regular nodes and HTTP nodes, including JVM total, used, and free memory, JVM thread count, and default time zone and locale.

To view node performance information:

1. On the Content DB Home page, click the name of the node for which you want to view performance information.
2. On the Node page, click the **Details** link to display operating system and JVM information about that node.

    Figure 9–2 shows the Details page.

Figure 9–2 Details Page for Selected Node



Page Refreshed **Jun 27, 2006 10:49:39 AM**

Java VM Total Memory (MB)	**65**
Java VM Used Memory (MB)	**60**
Java VM Free Memory (MB)	**5**
Java VM Thread Count	**83**
Java VM Default Time Zone	**PST8PDT**
Java VM Default Locale	**en_US**
IP Address	**stadf44.us.oracle.com/140.87.6.241**
Java Vendor	**Sun Microsystems Inc.**
Java Version	**1.4.2_06**
Java Home	**/cdb/mtm2/jdk/jre**
Operating System Name	**Linux**
Operating System Architecture	**i386**
Operating System Version	**2.4.21-37.ELsmp**
Content DB Version (beans-side)	**10.1.2.4.0**
Content DB Version (server-side)	**10.1.2.4.0**

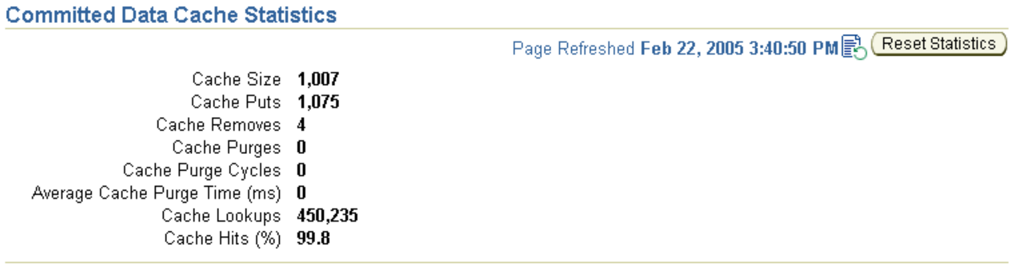
Monitoring Service Performance

You can view real-time statistics for the Committed Data Cache, the Read-Only Connection Pool, and the Writable Connection Pool for each service. You can also reset the statistics.

1. On the Content DB Home page, click the node whose service you want to monitor.
2. On the Node page, click the service (for example, **IfsDefaultService**).
3. On the Service page, scroll to the Performance section.
4. Click the link to the statistics you want to view: **Committed Data Cache Statistics** or **Connection Pool Statistics**.

   Figure 9–3 shows the Committed Data Cache Statistics page.

Figure 9–3 Committed Data Cache Statistics Page

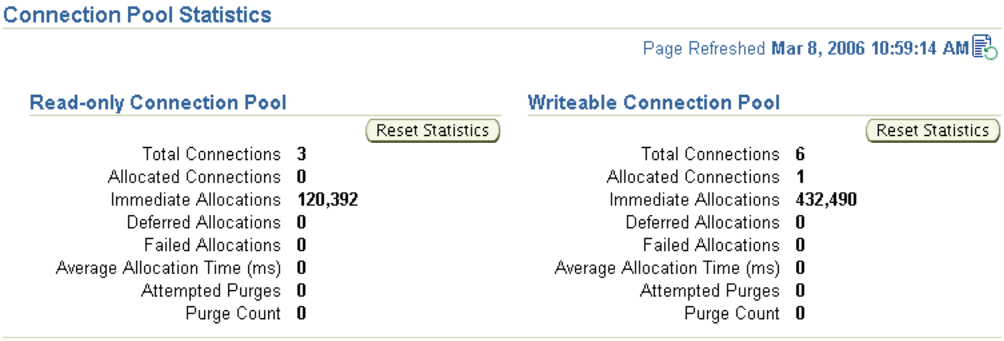


Page Refreshed **Feb 22, 2005 3:40:50 PM**

Cache Size	**1,007**
Cache Puts	**1,075**
Cache Removes	**4**
Cache Purges	**0**
Cache Purge Cycles	**0**
Average Cache Purge Time (ms)	**0**
Cache Lookups	**450,235**
Cache Hits (%)	**99.8**

Figure 9–4 shows the Connection Pool Statistics page.

Figure 9–4 Connection Pool Statistics Page



Page Refreshed Mar 8, 2006 10:59:14 AM

Read-only Connection Pool

Total Connections	3
Allocated Connections	0
Immediate Allocations	120,392
Deferred Allocations	0
Failed Allocations	0
Average Allocation Time (ms)	0
Attempted Purges	0
Purge Count	0

Writeable Connection Pool

Total Connections	6
Allocated Connections	1
Immediate Allocations	432,490
Deferred Allocations	0
Failed Allocations	0
Average Allocation Time (ms)	0
Attempted Purges	0
Purge Count	0

5. Click **Reset Statistics** in the Committed Data Cache, Read-Only Connection Pool, or Writeable Connection Pool areas to reset cache or connection pool statistics.

Logging Service Performance Information

The Statistics Agent captures the statistics for the Committed Data Cache, as well as the Read-Only and Writeable Connection Pools, and writes them to the node log and the application log. You can also configure this agent to write statistics to a document stored in the Oracle Content DB repository.

See "Viewing Logs" on page 9-7 for information about the node log and application log. See "Statistics Agent" on page E-16 for information about the Statistics Agent.

Monitoring Server Performance

You can monitor server performance by viewing Dynamic Monitoring Service (DMS) metrics that were defined for some servers. DMS metrics are a special type of performance metric that can be defined in Oracle Application Server. DMS metrics for Oracle Content DB include:

- WebDAV Servers
- FTP Servers
- Servers

Some DMS metric information can be viewed on the Node page, and on the Server page for some servers. For example, the Servers section of the Node page shows the Last Start Time and Last Stop Time for each server, while the FTP Server page displays Requests Completed, Average Request Processing Time (seconds), Downloaded Content Size (MB), and Uploaded Content Size (MB).

DMS metrics can also be viewed using the `dmstool` utility and AggreSpy. For more information about DMS metrics and how to view them, see *Oracle Application Server Performance Guide*.

Viewing Logs

The following sections provide a list of Oracle Content DB logs, and information about how to view logs in the Application Server Control.

Oracle Content DB Logs

Logs are generated by each node. Because some logs can get very large, manage your log files to ensure that you do not run out of disk space.

You can set the level of logging for various loggers, such as the FTP server, repository, or Web application, from the Configure Loggers page in the Application Server Control. See "Configuring Node Loggers" on page 8-12 for more information.

The Node Log

The node log records major state transitions (such as started, failed, or restarted) and provides centralized data on overall node health. This log is useful for troubleshooting protocol servers and agents. All errors are logged with stack traces. Log properties, such as Log Level and Rotation Interval, are specified in the node configuration of the node being monitored. The location of the node log cannot be changed. The node log is located in:

```
ORACLE_HOME/content/log/domain_name/node_name.log
```

You can also refer to the OPMN log for the regular node:

```
ORACLE_HOME/opmn/logs/Content~Node~1
```

The Application Log

The application log records additional information for HTTP nodes. This log is useful for troubleshooting the Oracle Content DB and Oracle Records DB applications and the WebDAV server. All errors are logged with stack traces. By default, application logs are located in:

```
ORACLE_HOME/j2ee/OC4J_Content/application-deployments/Content/OC4J_Content_
default_island_1/application.log

ORACLE_HOME/opmn/logs/Content~OC4J_Content~default_island~1

ORACLE_HOME/j2ee/OC4J_RM/application-deployments/rm/OC4J_RM_
default_island_1/application.log

ORACLE_HOME/opmn/logs/Content~OC4J_RM~default_island~1
```

Log for changehostname Script

When you run the `changehostname` script to change a middle-tier host name or IP address, a log is generated. This log is located in:

```
ORACLE_HOME/content/log/changehostname.log
```

Viewing Oracle Content DB Logs from the Application Server Control

You can view a variety of logs from the Application Server Control. This feature lets you view the logs without having to remember the individual log location.

To view log, click the **Logs** link in the upper-right corner of any Application Server Control page.

- The View Logs page provides a custom list of logs relevant to the component from where the link was clicked. For example, if you click **Logs** from any Oracle Content DB page, the View Logs page will display relevant Oracle Content DB logs, such as the node logs.

- You can also use Simple Search to locate logs. To do this, select the target that corresponds to the type of log you want to see from the **Available Components** list, and move it to the **Selected Components** list:
  - Select the Oracle Content DB instance (for example, **Content**) if you want to see the node log.
  - Select **OC4J_Content** or **OC4J_RM** to see the application log for Oracle Content DB or Oracle Records DB.
  - Select **Enterprise Manager** to see Application Server Control logs.

  Click **Search** to see the log names in the Results table.

Click the name of a log to see the log data. By default, the last 500 lines in the log appear in the log viewer. You can view up to 2000 lines. To download the contents of the entire log, click the log name at the top of the screen. If the log is large, the download may take several minutes.

Accessing Metrics and Monitoring Metric Alerts

You can access Oracle Content DB metrics from the Oracle Enterprise Manager 10*g* Grid Control. The following sections provide information about how to access the metrics and how to set up metric collection:

- Installing the Grid Control and Oracle Management Agent
- Setting the Management Agent Classpath
- Accessing the Grid Control
- Changing the Default Metric Collection Behavior
- Viewing Oracle Content DB Metrics in the Grid Control
- Metric Thresholds and Metric Collection Intervals

For more information about the metrics available for Oracle Content DB, click **Help** on any Grid Control Metrics page. For more information about the Grid Control, see *Oracle Enterprise Manager Concepts*.

> **Note:** The Grid Control uses "Oracle Content Services," the previous product name for Oracle Content DB, as the display name for Oracle Content DB targets.

Installing the Grid Control and Oracle Management Agent

Before you begin configuring the Grid Control to manage Oracle Content DB, you must install and configure the Grid Control on at least one host computer on your network. You can only use Grid Control 10*g* (10.2.0.2) with Oracle Content DB.

Oracle recommends that you install the Grid Control components on their own host or hosts. For example, if the Oracle Content DB middle tier is installed on `host1.us.oracle.com`, then install and configure the Oracle Management Service and Oracle Management Repository on `host2.us.oracle.com`.

You must install the Grid Control Oracle Management Agent on every Oracle Content DB host that you want to manage with the Grid Control.

See *Oracle Enterprise Manager Grid Control Installation and Basic Configuration* for more information.

Setting the Management Agent Classpath

To manage Oracle Content DB with Grid Control, you must run a script that is installed with the Management Agent. This script configures the Management Agent classpath so that the Management Agent can monitor the Oracle Content DB component.

To modify the Management Agent classpath:

1. Stop the Management Agent, if it has been started:
   - UNIX: `AGENT_HOME/bin/emctl stop agent`
   - Windows: `AGENT_HOME\bin\emctl stop agent`
2. Run the following command:
   - UNIX: `AGENT_HOME/files/emagent/bin/ifsemchgtarget`
   - Windows: `AGENT_HOME\files\emagent\bin\ifsemchgtarget`
3. When prompted, choose **4. Oracle Content Services Release 10.1.2**.

   (Oracle Content Services was the former product name for Oracle Content DB.)
4. Start the Management Agent:
   - UNIX: `AGENT_HOME/bin/emctl start agent`
   - Windows: `AGENT_HOME\bin\emctl start agent`

Accessing the Grid Control

To access the Grid Control, perform the following steps:

1. Use the following URL to access the Grid Control from a Web browser:

   http://*host_name*:*port*/em

   or

   https://*host_name*:*port*/em

   > **Note:** If you are uncertain about the port number, you can refer to one of the following files:
   >
   > - *ORACLE_HOME*/install/setupinfo.txt as displayed by the Oracle Universal Installer at the end of the installation
   > - *ORACLE_HOME*/install/portlist.ini on the Management Service computer

2. Log in as `sysman`, using the password you created during Oracle Enterprise Manager 10*g* installation. Or, log in as another Grid Control user with administrator privileges.

Changing the Default Metric Collection Behavior

You may want to enable or disable an Oracle Content DB metric for a middle-tier host after initial configuration. For example, you may want to enable the Load Balanced Application URL Timing metric on a middle tier because a load balancer has been recently added to the system, or you may want to disable the Application URL Timing metric on a middle tier because the HTTP node has been removed from that middle tier.

To change the default metric collection behavior, reconfigure the Oracle Content DB (`oracle_files`) targets for the given Oracle Content DB domain in the Grid Control.

> **Note:** In the following section, wherever you see "Oracle Content DB," the Grid Control displays "Oracle Content Services," the previous product name for Oracle Content DB.

Reconfiguring Oracle Content DB (oracle_files) Targets in the Grid Control

Follow these steps to change the default metric collection behavior of Oracle Content DB targets:

1. From the Grid Control Home page, click the **Targets** tab, then click the **All Targets** subtab. A list of all the discovered targets across the network appears.
2. Locate the Oracle Content DB target for the given middle tier. You can perform a quick search by entering the schema name in the **Search** field and clicking **Go**.
3. Select the Oracle Content DB target and click **Configure**.
4. Set the following values to `TRUE` or `FALSE` to enable or disable metric collection. The values must be in upper case.

   - **Run Repository Metric?**

     The default is `TRUE` for the first middle tier to be configured. For any additional Oracle Content DB middle tiers, the default is `FALSE`.

   - **Run Web Application Response Time Metric?**

     The default is `TRUE`. If you set this parameter to `TRUE`, specify a valid value for **Web Application URL**. If you sent this parameter to `FALSE`, enter `NULL` for **Web Application URL**.

   - **Run Load Balanced Web Application Response Time Metric?**

     The default is `FALSE`. If you set this parameter to `TRUE`, specify a valid value for **Load Balanced Web Application URL**. If you sent this parameter to `FALSE`, enter `NULL` for **Load Balanced Web Application URL**.

   - **Run RM Application Response Time Metric?**

     The default is `TRUE`. If you set this parameter to `TRUE`, specify a valid value for **RM Application URL** (in other words, the URL for the Oracle Records DB application). If you sent this parameter to `FALSE`, enter `NULL` for **RM Application URL**.

   - **Run Load Balanced RM Application Response Time Metric?**

     The default is `FALSE`. If you set this parameter to `TRUE`, specify a valid value for **Load Balanced RM Application URL** (in other words, the load-balanced URL for the Oracle Records DB application). If you sent this parameter to `FALSE`, enter `NULL` for **Load Balanced RM Application URL**.

   For more information about these parameters, click the **Help** link.
5. Click **OK**.

Viewing Oracle Content DB Metrics in the Grid Control

After you have logged in to the Grid Control, you can use the search function to navigate to the pages that show Oracle Content DB metrics.

To access Oracle Content DB metrics using the search function, follow these steps:

1. Click the **Targets** tab.
2. Click the **All Targets** subtab. A list of targets appears.
3. Type the name of your Oracle Content DB host in the **Search** field and click **Go**.
4. Click the name of your Oracle Content DB instance.
5. Click **All Metrics** to see a list of Oracle Content DB metrics.

Metric Thresholds and Metric Collection Intervals

You can use the Grid Control to edit the thresholds for Grid Control metrics. When you edit the thresholds, a customized collection file will be created in the following directory:

```
AGENT_HOME/sysman/emd/collection
```

For more information, see *Oracle Enterprise Manager Concepts*.

Metric Collection Intervals

You cannot use the Grid Control to update the metric collection intervals. If you must change the default intervals, you can manually edit the customized collection file described in the previous section. Do not specify a collection rate higher than once every minute, or it will have a negative impact on the performance of your entire system.

10

Managing Oracle Content DB Formats

Oracle Content DB associates a format (also known as a MIME type) with each document. You can add, modify, and delete formats using the Application Server Control.

This chapter provides information about the following topics:

- About Formats
- Adding Formats
- Modifying Formats
- Deleting Formats
- Default Formats

About Formats

The **format** of a document indicates the file type (for example, .doc or .zip). Oracle Content DB needs to know the format of documents to determine how to index their content. In addition, the Documents tab of the Domain Performance & Statistics page in the Application Server Control provides information about documents according to their MIME type.

A format contains the following information:

- **MIME type:** Specifies the type of content stored in Oracle Content DB, such as `text/plain` or `text/html`.
- **Extension type:** Specifies the default extension for files that use this format, such as `.fm` or `.jar`.
- **Binary setting:** Determines whether files that use this format are of binary type.
- **Index setting:** Determines whether files that use this format need to be indexed.
- **Omitted From Antivirus Scan:** Determines whether files that use this format need to be omitted from antivirus scans.

Indexing a format type is the basis of content searching in Oracle Content DB. If a format is not indexed, content searches will fail. Content searches can also fail when formats are indexed incorrectly.

See Appendix B, "Oracle Text Supported Document Formats" in *Oracle Text Reference* for information about which formats can be indexed by Oracle Text.

Adding Formats

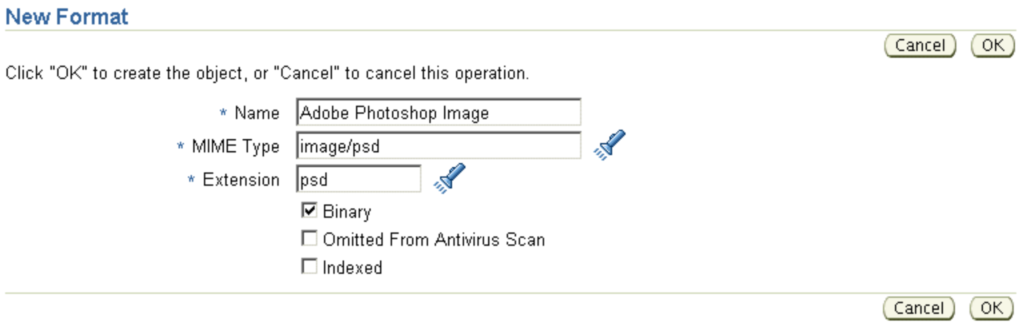
You can add more formats to Oracle Content DB for special types of content. See "Default Formats" on page 10-3 for a list of default formats.

To add a format:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Formats**.
3. On the Formats page, click **New Format**. The New Format page appears.

   Figure 10–1 shows the New Format page.

Figure 10–1 New Format Page


New Format

Click "OK" to create the object, or "Cancel" to cancel this operation.

* Name: Adobe Photoshop Image

* MIME Type: image/psd

* Extension: psd

☑ Binary

☐ Omitted From Antivirus Scan

☐ Indexed

4. Enter the following information:
   - **Name:** Provide a name for the format (for example, FrameMaker or Jar).
   - **MIME Type:** Specify the type of content stored in Oracle Content DB, such as `text/plain` or `text/html`. Click the Flashlight icon to select from a list of MIME types.
   - **Extension:** Specify the default extension for files that use this format, such as `.fm` or `.jar`. Click the Flashlight icon to select from a list of file extensions.
   - **Binary:** Specify whether files that use this format are of binary type.
   - **Omitted From Antivirus Scan:** Specify whether files that use this format need to be omitted from antivirus scans.
   - **Indexed:** Specify whether files that use this format need to be indexed.
5. Click **OK**.

Modifying Formats

You can modify formats using the Application Server Control. The Unknown format is a required system format and cannot be modified.

To modify a format:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Formats**.
3. On the Formats page, click the name of the format you want to modify.
4. On the Edit Format page, you can change the following information:

- **MIME Type:** Specify the type of content stored in Oracle Content DB, such as `text/plain` or `text/html`. Click the Flashlight icon to select from a list of MIME types.
- **Extension:** Specify the default extension for files that use this format, such as `.fm` or `.jar`. Click the Flashlight icon to select from a list of file extensions.
- **Binary:** Specify whether files that use this format are of binary type.
- **Omitted From Antivirus Scan:** Specify whether files that use this format need to be omitted from antivirus scans.
- **Indexed:** Specify whether files that use this format need to be indexed. Changing this setting only affects new documents that are uploaded to Oracle Content DB; the index setting for existing documents that use this format will not be changed. To force indexing of existing documents, upload the documents again after changing this setting.

5. Click **OK**.

Some formats must be indexed. For these formats, the index setting cannot be changed.

Deleting Formats

You can delete formats using the Application Server Control. The Unknown format is a required system format and cannot be deleted.

To delete a format:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Formats**.
3. On the Formats page, select the format you want to delete.
4. Click **Delete**.
5. When asked to confirm the deletion, click **OK**.

Default Formats

Table 10–1 provides a list of default formats.

Table 10–1 Default System Formats

Format Name	Extension	Indexed by Default?	Can Change Index Setting?[1]
Advanced Stream Redirector File	asx	No	Yes
Advanced Streaming Format	asf	No	Yes
Apple Quicktime	mov	Yes	No
Apple Quicktime (qt)	qt	Yes	No
Audio Interchange File (aif)	aif	Yes	No
Audio Interchange File (aifc)	aifc	Yes	No
Audio Interchange File (aiff)	aiff	Yes	No
Basic audio	au	Yes	No
Bitmap image	bmp	Yes	No

Table 10–1 (Cont.) Default System Formats

Format Name	Extension	Indexed by Default?	Can Change Index Setting?[1]
c file	c	Yes	Yes
C Header	h	Yes	Yes
C++ Header (h++)	h++	Yes	Yes
C++ Header (hh)	hh	Yes	Yes
C++ Header (hpp)	hpp	Yes	Yes
C++ Header (hxx)	hxx	Yes	Yes
C++ Source Code (C++)	c++	Yes	Yes
C++ Source Code (cc)	cc	Yes	Yes
C++ Source Code (cpp)	cpp	Yes	Yes
CC++ Source Code (cxx)	cxx	Yes	Yes
Comma-Separated Values	csv	Yes	Yes
Compiled WML Document	wmlc	No	Yes
Compiled WML Script	wmlsc	No	Yes
Compressed File	taz	No	Yes
Corel Photo-Paint Image	cpt	No	Yes
Corel Vector Graphic Drawing	cdr	No	Yes
Corel Vector Pattern	pat	No	Yes
CorelDraw Template	cdt	No	Yes
Debian Linux Package	deb	No	Yes
Difference File	diff	Yes	Yes
Email Message	eml	Yes	No
Encapsulated PostScript	eps	Yes	Yes
Extensible HyperText Markup Language File	xhtml	Yes	Yes
Extensible Markup Language	xml	Yes	Yes
FileMaker Pro Spreadsheet	fm	Yes	Yes
FrameMaker Book	book	Yes	Yes
FrameMaker FBDOC	fbdoc	Yes	Yes
FrameMaker FRAME	frame	Yes	Yes
FrameMaker FRM	frm	Yes	Yes
FrameMaker MAKER	maker	Yes	Yes
GIF	gif	Yes	No
GNU tar Compressed File Archive (GNU Tape Archive)	gtar	No	Yes
GZIP	gz	No	Yes
HTML	htm	Yes	Yes
HTML unix	html	Yes	No

Table 10–1 (Cont.) Default System Formats

Format Name	**Extension**	**Indexed by Default?**	**Can Change Index Setting?**[1]
Hypertext Cascading Style Sheet	css	Yes	Yes
JAR	jar	No	Yes
Java Bytecode	class	No	Yes
java file	java	Yes	Yes
Java Serialized Object File	ser	No	Yes
JavaScript Source Code	js	Yes	Yes
JNLP	jnlp	No	Yes
JPEG	jpg	Yes	No
JPEG (jpe)	jpe	Yes	No
JPEG (jpeg)	jpeg	Yes	No
JSP	jsp	Yes	Yes
Lotus 123 Spreadsheet	wk	Yes	Yes
Macintosh Sound Resource	snd	No	Yes
Macromedia Director Movie	dir	No	Yes
Macromedia Director Protected Movie File	dxr	No	Yes
Macromedia Flash Format File	swf	No	Yes
Macromedia Flash Format File - swfl	swfl	No	Yes
MHTML Document mhtm	mht	Yes	Yes
MHTML Document mhtml	mhtml	Yes	Yes
Microsoft AVI	avi	Yes	No
Microsoft PowerPoint	ppt	Yes	Yes
Microsoft Powerpoint (pot)	pot	Yes	Yes
Microsoft Powerpoint Show	pps	Yes	Yes
Microsoft Wave Audio	wav	Yes	No
MIDI	mid	No	Yes
Money Data File	mny	No	Yes
MP3 Playlist File	m3u	No	Yes
MPEG	mpg	No	Yes
MPEG (mpe)	mpe	No	Yes
MPEG (mpeg)	mpeg	No	Yes
MPEG - mpega	mpega	Yes	No
MPEG Layer 2	mp2	Yes	No
MPEG Layer 3 Audio	mp3	Yes	No
MPEG Layer 3 Audio Stream	mpga	Yes	No
MS Access	mdb	Yes	Yes
MS DOS Batch Processing	bat	Yes	Yes

Table 10–1 (Cont.) Default System Formats

Format Name	Extension	Indexed by Default?	Can Change Index Setting?[1]
MS Excel	xls	Yes	Yes
MS Excel (xlb)	xlb	Yes	Yes
MS Executable File	exe	No	Yes
MS Windows Dynamic Link Library	dll	No	Yes
MS Word	doc	Yes	Yes
MS Word (dot)	dot	Yes	Yes
MS Works	msw	Yes	Yes
Object File	o	No	Yes
OpenOffice.org Drawing	sda	No	Yes
OpenOffice.org Presentation	sdd	Yes	Yes
Outlook Express News File	nws	No	Yes
PCX	pcx	No	Yes
PDF	pdf	Yes	Yes
PERL Program File	pl	Yes	Yes
Portable (Public) Network Graphic	png	No	Yes
portable pixmap	ppm	No	Yes
Postscript	ps	No	Yes
postscript-ai	ai	No	Yes
Project File	mpp	Yes	Yes
Real Audio (ra)	ra	Yes	No
Real Audio (ram)	ram	Yes	Yes
Real Media (rm)	rm	Yes	No
Real Video	rv	Yes	No
RedHat Package Manager	rpm	No	Yes
RichText	rtf	Yes	Yes
RichText (rtx)	rtx	Yes	Yes
Schedule/Schedule+ Data	scd	No	Yes
SGI Video	movie	No	Yes
Shell Script	sh	Yes	Yes
Shockwave Movie	dcr	No	Yes
Sourcecode	src	Yes	Yes
Standard General Markup Language	sgml	Yes	Yes
Tab Separated Values File	tsv	Yes	Yes
Tar	tar	No	Yes
Tcl (Tool Command Language) Language Script	tcl	Yes	Yes
Text	txt	Yes	Yes

Table 10–1 (Cont.) Default System Formats

Format Name	Extension	Indexed by Default?	Can Change Index Setting?[1]
Text Document (text)	text	Yes	Yes
TIFF	tif	Yes	No
TIFF (tiff)	tiff	Yes	No
Tk Language Script	tk	Yes	Yes
UNIX Compressed Archive File	z	No	Yes
UNIX csh Shell Script	csh	Yes	Yes
UNIX Tar File Gzipped	tgz	No	Yes
Unknown	(N/A)	No	No
Unknown Binary	bin	No	Yes
URL Reference	url	No	Yes
vCalendar File	vcs	No	Yes
vCard File	vcf	Yes	Yes
Visio Drawing	vsd	Yes	Yes
VRML	vrml	No	Yes
Windows Help File	hlp	No	Yes
Windows Icon	ico	No	Yes
Wireless Markup Language File	wml	Yes	Yes
WML Script	wmls	Yes	Yes
Word Perfect	wpd	Yes	Yes
Wordperfect 5.1 Document	wp5	Yes	Yes
XFIG Graphic File	fig	No	Yes
xpixmap	xpm	No	Yes
xpixmap pm	pm	No	Yes
Zip	zip	No	Yes

[1] Some formats must be indexed. For these formats, the index setting cannot be changed.

11

Managing Oracle Content DB Sites

In Oracle Content DB, a **Site** is a discrete organizational entity whose users can collaborate on files and folders. Users in one Site do not have access to the content of users in another Site. Each Site has an allocated quota that specifies the amount of content (in MB, GB, or TB) that can be stored in the Site. Oracle Content DB Sites are based on **identity management realms**.

You can use the Application Server Control to create new Sites, or enable, disable, modify, or delete existing Sites. You can also grant the Security Administrator role to a particular Site user.

This chapter provides information about the following topics:

- About Sites
- Creating Sites
- Modifying Sites
- Granting the Security Administrator Role
- Enabling and Disabling Sites
- Deleting Sites

About Sites

Oracle Content DB Sites are based on realms that were defined in Oracle Identity Management. A realm is a collection of identities and associated policies that is typically used when enterprises want to isolate user populations and enforce different identity management policies for each population.

Each installation of Oracle Content DB has a default Site, based on the default realm in Oracle Identity Management.

Important: If you want to choose another realm as the default, or if you want to change the name of the default realm, you must make the change before you install and configure Oracle Content DB. You cannot change the default realm or realm name after Oracle Content DB has been installed and configured.

You can create and manage additional realms using the Oracle Internet Directory Self-Service Console. You must configure OracleAS Single Sign-On for multiple realms if you want to have more than one realm in your deployment. For information about how to do this, see S*Oracle Application Server Single Sign-On Administrator's Guide*.

There are a number of application administrators for each Site who perform functions such as allocating quota and assigning roles. The application administration roles include the User Administrator, Content Administrator, and Quota Administrator. For more information about the application administrator roles and tasks, see *Oracle Content Database Application Administrator's Guide*.

Each Site has an allocated quota that specifies the amount of content (in MB, GB, or TB) that can be stored in the Site. When the quota consumed by a Site reaches 95 percent of the allocated quota, an e-mail notification is sent to the administrator e-mail address, and to any users of that Site with the Quota Administrator role. The administrator e-mail address is specified in the `IFS.DOMAIN.EMAIL.AdministratorAddress` domain property. See "Changing Domain Properties" on page 8-1 for information about how to specify this administrator e-mail address.

Quota warning e-mail notifications are issued by the Cleanup Agent. You can change the properties of this agent to adjust the warning threshold, or to specify whether files in the **Archive** count against Site quota. These properties are not Site-specific; they apply to all the Sites in your deployment. See "Cleanup Agent" on page E-4 for more information about these properties.

Creating Sites

Each new Site that you create must be based on an existing realm; if all the realms have been used for other Sites, you must create a new realm in Oracle Internet Directory before you can create a new Site.

To create a new Site:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Sites**.
3. On the Sites page, click **Create**.
4. In the **Name** field, provide a name for the new Site.

   Oracle recommends that you use the name of the realm on which this Site will be based for the name of the Site. Because users for this Site will need to provide the realm name during authentication, having the Site name based on the realm name provides consistency.

   The Site name is used as the top folder name for the new Site and will appear in all Site paths. Because of this, you cannot use the following characters in the Site name: backslash (\), slash (/), colon (:), asterisk (*), question mark (?), quotation mark ("), left angle bracket (<), right angle bracket (>), and vertical bar (|). Keep Site names short to avoid long path names, and avoid using spaces because these characters will be replaced by %20 in URLs, making the URL long and hard to read.
5. For **Realm**, select a realm on which you want to base the new Site.
6. Specify an **Allocated Quota** for the new Site, in megabytes (MB), gigabytes (GB), or terabytes (TB).
7. Specify whether you want the new Site to be enabled by default. Disabled Sites cannot accept new user sessions.
8. Click **OK**.
9. Return to the Content DB Home page and restart **OC4J_Content**. If you are using Oracle Records DB, you must also restart **OC4J_RM**. If you are running these

processes on multiple middle tiers, you must restart these processes on all middle tiers.

If you need to change the default location of the Personal Libraries for new users of this Site, modify the Site after it has been created, and specify the required properties. See the following section for more information.

Modifying Sites

You can change settings for existing Sites, including changing the Site name, updating Site quota, and changing the location of Personal Libraries for new users.

To modify an existing Site:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Sites**.
3. Click the name of the Site you want to modify.
4. If necessary, provide a new name for the Site. Since the Site name is used as the top folder name for the Site, any bookmarks to existing URLs will break. Also, in Oracle Drive, any paths designated for scheduled backups will need to be changed.

   You cannot use the following characters in the Site name: backslash (\), slash (/), colon (:), asterisk (*), question mark (?), quotation mark ("), left angle bracket (<), right angle bracket (>), and vertical bar (|). Keep Site names short to avoid long path names, and avoid using spaces because these characters will be replaced by %20 in URLs, making the URL long and hard to read.
5. Specify the amount of quota you want to allocate in the **Allocated Quota** field, then specify whether you want to allocate the quota in Megabytes (MB), Gigabytes (GB), or Terabytes (TB) by selecting from the list. The quota you allocate must be larger than the quota that has already been used by the Site.
6. In the Personal Libraries section, you have the option of changing the location of the Personal Libraries for new users. Using this option requires custom Java code; contact your Oracle Support Services representative for more information. To change the location of the Personal Libraries for new users, provide the following two parameters:

   - **Locator Class Name:** Specify the name of the custom class you created for the new Personal Library location.
   - **Root Path:** Specify the new root path for the Personal Libraries.

   Only the Personal Libraries for new users will use the new path. Personal Libraries for existing users will remain in the old location.
7. Click **OK**.

Granting the Security Administrator Role

If all existing Site users with the Security Administrator role are deleted or deprovisioned, you can use the Application Server Control to grant the Security Administrator role to a Site user.

For more information about the Security Administrator role, see *Oracle Content Database Application Administrator's Guide*.

To grant the Security Administrator role to a Site user:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Sites**.
3. Select the Site where you want to grant Security Administrator access.
4. Click **Grant Security Role**.
5. On the Grant Security Role page, enter the name of the user to whom you want to grant the Security Administrator role.
6. Click **OK**.

Enabling and Disabling Sites

You can choose whether to enable or disable Sites. Disabled Sites cannot accept new user sessions.

To enable a Site:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Sites**.
3. Select the Site you want to enable and click **Enable**.
4. On the Warning page, click **Yes**.

To disable a Site:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Sites**.
3. Select the Site you want to disable and click **Disable**.
4. On the Warning page, click **Yes**.
5. After you disable a Site, it will not accept any new sessions. To terminate existing sessions, return to the Content DB Home page and click **Restart Domain**.

Deleting Sites

Delete a Site only if you are sure that you will not need to access anything in the Site again. When a Site is deleted, all content and associated metadata is deleted. The Containers, Libraries, users, groups, roles, categories, and the Archive for the Site are also deleted. You cannot delete the default Site.

To delete a Site:

1. Connect to the Application Server Control and go to the Content DB Home page.
2. In the Administration section, click **Sites**.
3. If the Site you want to delete is enabled, select the Site and click **Disable**. Then, on the Warning page, click **Yes**. Enabled Sites cannot be deleted.
4. Select the Site and click **Delete**. Then, on the Warning page, click **Yes**. Everything associated with that Site, including content, metadata, users, and Libraries, is deleted, and the Site is removed from the Sites list.

You cannot delete a Site that contains records. See *Oracle Records Database Administrator's Guide* for information about managing records.

12

Oracle Content DB Maintenance and Tuning

This chapter provides information about ongoing system maintenance, performance tuning, and recovery. As with any production system, your implementation of Oracle Content DB needs to include a basic disaster recovery plan.

This chapter provides information about the following topics:

- Backup and Recovery
- Service Configurations and Java Memory Sizing
- Performance Tuning
- Analyzing Performance Problems

Backup and Recovery

Always back up the system before upgrading, migrating new data, or making other major changes:

- **Oracle Database tier:** See *Oracle Database Backup and Recovery User's Guide* for complete information about backing up Oracle Database. In addition, note the following:
  - In addition to the Oracle Content DB schema, there are two special schemas that ensure secure connectivity to other systems: `CONTENT$CM` and `CONTENT$ID`. When you back up your system, make sure to include these schemas.
  - Make sure to back up the Oracle Workflow schema, `OWF_MGR`.
  - If you use BFILEs, make sure to back them up also.
- **OracleAS Infrastructure tier:** Refer to *Oracle Application Server Administrator's Guide* for information about backing up and restoring OracleAS Infrastructure.
- **Oracle Content DB middle tier:** There is no backup and recovery tool for the middle tier. To back up the middle tier, make a complete copy of the Oracle home. Also, make a copy of the `oraInventory` directory on the middle-tier computer.

Service Configurations and Java Memory Sizing

In Oracle Content DB, the default service configurations specify the maximum number of Library **sessions** that can connect to the service. Restricting the number of Library sessions reduces the likelihood of getting out of memory errors in the `OC4J_Content.default_island.1` or in the `application.log` files.

In previous releases, the default service configurations allowed an unlimited number of sessions. Due to this change, you may see the following errors:

- Oracle Content DB Web client: "The maximum number of concurrent sessions has been reached. Please try your request again later."
- `OC4J_Content.default_island.1` or `application.log`: "IFS-20127: Service too busy (maximum concurrent sessions)"

If you see either error, change the service configuration from small to medium or from medium to large, or create a custom service configuration. If you use the large service configuration, or if you create a custom service configuration, you must adjust your `-Xmx` setting.

If you see `java.lang.OutOfMemory` errors in your `OC4J_Content.default_island.1` or `application.log` files, then you also need to adjust your `-Xmx` setting.

Table 12–1 describes factors that might require you to change the `-Xmx` setting.

Table 12–1 Xmx Settings

Service Configuration	Setting for IFS.SERVICE. Maximum ConcurrentSessions	Expected PCCU	Recommended Size for Xmx (Java Maximum Memory)	Need to change the default Xmx setting of 256MB?
Small	40	25	64 MB	No
Medium	70	45	162 MB	No
Large	200	125	430 MB	**Yes**

Note: The term PCCU refers to Peak Concurrent Connected Users. PCCU is the number of users who are signed on to Oracle Content DB and have performed an operation during the peak hour of the day. If you do not know the number of peak hour users, assume 10 percent of your Oracle Content DB user population.

See "Managing Service Configurations" on page 8-14 for additional information about creating and changing service configurations.

Calculating Xmx Settings

A general guideline for calculating the `Xmx` setting is:

```
Xmx = PCCU * 2.8MB
```

Alternatively, you can use the following equation to determine a more precise value:

```
Xmx = (PCCU * 1.6 sessions per PCCU * 1MB per session) + (DATACACHE.Size * 3KB per
data cache object) + (20% JVM overhead for garbage collection)
```

The maximum value for the `Xmx` setting depends on your operating system. On Linux operating systems, the setting cannot exceed 2GB. On Solaris operating systems, the setting cannot exceed 4GB. Oracle recommends that the `Xmx` setting does not exceed 2GB for Oracle Content DB.

See "Modifying Node Configurations" on page 8-8 for more information about how to change the `Xmx` setting.

Adjusting Service Configuration Settings

If you expect that your peak concurrent connected users (PCCU) will exceed 125, create a custom service configuration using the following recommendations:

```
MaximumConcurrentSessions = 1.6 * PCCU
DATACACHE.Size = 400 * PCCU
DATACACHE.EmergencyTrigger = 0.80 * DATACACHE.Size
DATACACHE.UrgentTrigger = 0.75 * DATACACHE.Size
DATACACHE.NormalTrigger = 0.65 * DATACACHE.Size
DATACACHE.PurgeTarget = 0.55 * DATACACHE.Size
CONNECTIONPOOL.WRITEABLE.MaximumSize = 0.05 * PCCU
CONNECTIONPOOL.WRITEABLE.TargetSize = 0.04 * PCCU
CONNECTIONPOOL.WRITEABLE.MinimumSize = 5
CONNECTIONPOOL.READONLY.MaximumSize = 0.05 * PCCU
CONNECTIONPOOL.READONLY.TargetSize = 0.04 * PCCU
CONNECTIONPOOL.READONLY.MinimumSize = 5
```

The other settings in the service configuration generally do not need to be adjusted.

Performance Tuning

Performance is typically affected by network I/O, hard-disk drive I/O, memory (random access memory) I/O, or some combination of these three or other factors. Adjusting one of the factors sometimes moves the performance problem to a new location, so you must approach the tuning task in a logical manner.

In addition to the information provided in the following section, see "Storing Files in an Oracle Database" on page 2-11 and "Oracle Content DB Metadata and Infrastructure" on page 2-12 for information about how to calculate the appropriate space for document storage.

See *Oracle Database Performance Tuning Guide* for complete information about performance tuning.

Running the Oracle Content DB analyze.sql Script

Oracle Content DB uses Oracle Database Cost-Based Optimizer (CBO) to determine the most efficient way to run SQL statements. For the CBO to work properly, the Oracle Content DB `analyze.sql` script needs to be run as part of regular Oracle Content DB operations, especially after large volume changes to the data, such as after users have loaded a large number of files into the database instance. This script generates statistics about the distribution of data in Oracle Content DB so that the CBO can choose the most efficient way to execute SQL statements. For more information about the Cost-Based Optimizer, see *Oracle Database Performance Tuning Guide*.

Run the script during periods that are not busy to avoid impeding system performance.

The `analyze.sql` script, which makes calls to the `DBMS_STATS` package, exports schema statistics to a backup table, so you can restore statistics later, if necessary, as discussed in "Restoring Prior Statistics" in the following section. To run the script, enter the following at the command line:

```
cd ORACLE_HOME/content/admin/sql
sqlplus content_db_schema/password@connect_string @analyze.sql content_db_schema
```

This script may take a while to run, especially if Oracle Content DB contains a large number of documents.

Restoring Prior Statistics

Before gathering new statistics, the `analyze.sql` script exports backup statistics to the `IFS_BACKUP_STATS` table, marking the set of statistics with a time stamp. You can query the table for existing saved sets by running this SQL statement:

```
SQL> select distinct statid from IFS_BACKUP_STATS;
```

This query returns a list of all statistics by statistic ID (the date and time stamp). For example:

```
STATID
------------------------------
01-MAY-02 02:15.36
04-MAY-02 20:00.15
08-MAY-02 02:15.48
11-MAY-02 06:21.40
11-MAY-02 20:15.37
```

You can then restore the statistics from a day and time when you know performance was better. For example, if you find that after using the statistics from the 8:00 p.m. run of the `analyze` script that performance is worse, then you can restore the statistics from earlier that day using:

```
SQL> call dbms_stats.import_schema_stats (content_db_schema,
'IFS_BACKUP_STATS', '08-MAY-02 06:21.40',content_db_schema);
```

By restoring the statistics, you are directing the CBO to revert to the way it previously ran SQL statements.

Analyzing Performance Problems

After ensuring that you have run statistics properly and have enough free hard-disk space to support the tablespaces, you may still have performance problems. If you have performance problems, you must determine whether the performance bottleneck is caused by Oracle Database, Oracle Content DB, or other factors.

To isolate the problem, start looking at which processes are running and how many resources they are using:

1. Run `top` (on UNIX) or start the Task Manager (on Windows platforms) as you reproduce the problem.
2. Determine whether a Java process, the Oracle shadow process, I/O, or a combination is the bottleneck during that time.

If the Database Is Causing the Problem

If the problem is the Oracle shadow process, use the Statspack utility to determine the SQL statement that is causing the largest number of buffer gets, and run Explain Plan on it.

If you see full table scans, then that may be the cause of the problem; the optimizer may not be choosing an appropriate plan. Report that problem to Oracle Support Services. Additional work must be done to isolate the problem.

For more information about the Statspack utility and Explain Plan, see *Oracle Database Performance Tuning Guide*.

If the Java Processes Are Causing the Problem

You may not have enough memory. For example, if you see any `java.lang.OutOfMemoryError` errors in your logs, increase your maximum memory (`Xmx`) settings for that JVM. See "Modifying Node Configurations" on page 8-8 for more information about changing the `Xmx` setting.

If users are experiencing poor response times, and `top` (on UNIX) or its equivalent (for example, Task Manager on Windows platforms), shows a Java process running at 100 percent of a CPU for a minute or longer, then the `Xmx` setting for Java may be too small.

1. Turn on verbose garbage collection (`verbosegc`). To do this, edit the Java Properties of the node configuration. See Table 8–2, " Node Configuration Properties" on page 8-9 for more information.

   In the node log file, output related to garbage collection appears as follows:

   ```
   [Full GC 1476K->1476K(2112K), 0.0549430 secs]
   ```

   A Full GC occurs when the Garbage Collector has exhausted all available memory in the nursery, and has to go into the rest of the heap to reclaim memory.

2. If Full GCs occur more than once every 10 minutes (not just after startup), increase your `Xmx` settings for that JVM.

Viewing Cache Statistics and Changing Cache Settings

If the problem is an Oracle Content DB Java process, start by checking the percentage of cache hits for the Oracle Content DB service using the Application Server Control, as follows:

1. On the Content DB Home page, click the name of the node you want to manage.
2. Click the name of the service. Typically, this will be `IfsDefaultService`. The Service page appears.
3. Scroll to the Performance section and click **Committed Data Cache Statistics**. The Committed Data Cache Statistics page appears, showing real-time data for Cache Size, Cache Puts, Cache Removes, Cache Purges, Cache Purge Cycles, Average Cache Purge Time (ms), Cache Lookups, and Cache Hits (%).

   The goal is to have a high percentage of Cache Hits; as much as 100 percent is possible. If the percentage of Cache Hits for the service is less than 98 percent, the size of the Committed Data Cache may be too small.

   Because the Statistics Agent captures the real-time data, you can also see prior statistics by viewing the node log or application log. You can also configure this agent to write statistics to a document stored in the Oracle Content DB repository. See "Statistics Agent" on page E-16 for information about the Statistics Agent.

4. To change the run-time Cache settings, return to the Service page and, in the Administration section, click **Committed Data Cache Administration**.
5. Proportionately increase all Cache settings (Cache Capacity, Normal Purge Trigger, Urgent Purge Trigger, Emergency Purge Trigger, Purge Target) and click **Apply**.

   This will increase your memory usage on the middle tier computer by approximately 3 KB for each object. For example, if you increase cache capacity by 5000, your memory usage will grow by 15 MB.

To make the changes permanent, update the service configuration. See "Modifying Service Configurations" on page 8-16 for more information.

Viewing Connection Pool Statistics and Changing Connection Pool Settings

Check the target and maximum number of connections for the Read-Only and Writable Connection Pools using the Application Server Control, as follows:

1. On the Content DB Home page, click the name of the node you want to manage.
2. Click the name of the service. Typically, this will be `IfsDefaultService`. The Service page appears.
3. Scroll to the Performance section and click **Connection Pool Statistics**.

   Increase the Target Maximum Number of Connections and Absolute Maximum Number of Connections if any of the following is true:

   - Failed Allocations is greater than zero.
   - Total Connections is more than two higher than Target Maximum Number of Connections.
   - Deferred Allocations is greater than 5 percent, and Average Allocation Time (ms) is more than 10 milliseconds.

   Because the Statistics Agent captures the real-time data, you can also see prior statistics by viewing the node log or application log. You can also configure this agent to write statistics to a document stored in the Oracle Content DB repository. See "Statistics Agent" on page E-16 for information about the Statistics Agent.
4. To change the run-time Connection Pool settings, return to the Service page and, in the Administration section, click **Connection Pool Administration**.
5. Increase the **Target Maximum Number of Connections** and **Absolute Maximum Number of Connections**, and click **Apply**.

   Each additional Target or Absolute connection will use approximately 8 MB for each connection on the middle tier and 1 MB for each connection on the database.

To make the changes permanent, update the service configuration. See "Modifying Service Configurations" on page 8-16 for more information.

A

Troubleshooting Oracle Content DB

Use this appendix to troubleshoot problems in your Oracle Content DB installation.

This appendix provides information about the following topics:

- Solving General Administration Problems
- Solving Problems with Oracle Content DB Protocols
- Solving Performance Problems

Solving General Administration Problems

Table A–1 provides information about how to troubleshoot general Oracle Content DB administration problems.

Table A–1 General Administration Issues

Problem	Probable Cause	Corrective Action
Cannot connect to Oracle Content DB.	The Oracle Content DB server may be using DHCP.	If Oracle Content DB is using DHCP, use the current IP address of the server to connect, rather than the host name. All Oracle Content DB protocols are affected, including HTTP.
Users fail to be provisioned, or newly provisioned users cannot be added to Libraries.	Required user attributes were not set in Oracle Internet Directory.	The following Oracle Internet Directory user attributes must be nonnull for all users: `sn`, `givenName`, `mail`. In addition, all users must have a nonnull user name. The user name is specified by the `orclCommonNickname Attribute` in the OracleContext of the realm. See *Oracle Internet Directory Administrator's Guide* for more information about viewing the `orclCommonNicknameAttribute`.
Users cannot access Properties dialog boxes or other dialog boxes in the Oracle Content DB or Oracle Records DB Web clients.	Pop-up blockers are blocking these application dialog boxes.	Users must disable pop-up blockers to access some features of the Oracle Content DB and Oracle Records DB Web clients. Users should hold down the Ctrl key while clicking Launch to bypass most pop-up blockers. In addition, users can refer to the Help for the browser for more information about pop-up settings.
Content queries through the Web and Windows return no rows.	Oracle Text indexing of the documents has not occurred.	See "Maintaining the IFS_TEXT Index by Using the Oracle Text PL/SQL Packages" on page C-2 for more information.
Cannot log in as `cn=orcladmin`.	You forgot or do not know the `cn=orcladmin` password.	You can reset the password in the Metadata Repository database. The DSE root attribute name is `orclsupassword`. **Note:** After a certain number of failed attempts to connect, the `cn=orcladmin` account becomes locked. In this case, you must unlock the account.

Table A–1 (Cont.) General Administration Issues

Problem	Probable Cause	Corrective Action

The `cn=orcladmin` account becomes locked.	The `cn=orcladmin` account becomes locked, by default, after 10 failed attempts to connect. This setting is controlled by the password policy.	If you know the `cn=orcladmin` password, you can unlock the account by running the following command from the OracleAS Infrastructure Oracle home:
		`ORACLE_HOME/bin/oidpasswd connect=db_SID unlock_su_acct=true`
		In the preceding comamnd, *`db_SID`* is the SID for the database. For example:
		`ORACLE_HOME/bin/oidpasswd connect=orcl unlock_su_acct=true`
		`OID DB user password: my_ODS_password`
		`OID superuser account unlocked successfully.`
		The command prompts for the password of the ODS schema. By default, the ODS password is the same as for the `cn=orcladmin` account, which was set during OracleAS Infrastructure installation.
		See Also: *Oracle Internet Directory Administrator's Guide* for information about changing the password policy for the allowed number of failed attempts to connect

The password for the `cn=orcladmin` account has expired, and you want to change the default password expiration time.	The default password expiration time is 60 days.	To change the default expiration time for the `cn=orcladmin` password:
		1. If the `cn=orcladmin` account is locked, you must unlock the account before you can modify the password policy. See the preceding item in this table for more information.
		2. Log in to Oracle Directory Manager and go to Password Policy Management.
		3. Look for the following two attributes:
		- The `PasswordExpiryTime` attribute under the `cn=PwdPolicyEntry` (for example, `password_policy_entry,dc=mycompany,dc=com`)
		- The `pwdmaxage` attribute under Entry Management (for example, `cn=PwdPolicyEntry,cn=common,cn=products,cn=OracleContext,dc=mycompany,dc=com`)
		4. Change the `pwdmaxage` attribute in each password policy to an appropriate value. For example:
		5184000 = 60 days (default)
		7776000 = 90 days
		10368000 = 120 days
		15552000 = 180 days
		31536000 = 1 year
		Note: It is very important to change this value in both places.
		5. Still in Oracle Directory Manager, go to the realm-specific `orcladmin` account. Find the `userpassword` attribute and assign a new value. You can then start any Oracle component that uses OracleAS Single Sign-On and log in as `orcladmin`.
		6. Run the `odisrvreg` utility to reset the randomly generated password for Oracle Directory Integration and Provisioning. For example:
		`odisrvreg -D cn=orcladmin -w mypassword -p 3060`
		`Already Registered...Updating DIS password...`
		`DIS registration successful.`
		See Also: *Oracle Identity Management Integration Guide* for more information

An out-of-memory exception occurs when running Oracle Content DB.	The maximum Java heap size is too low.	Increase the heap size by modifying the `-Xmx` setting for that node configuration. See "Modifying Node Configurations" on page 8-8 for more information.

Table A–1 (Cont.) General Administration Issues

Problem	Probable Cause	Corrective Action

Need to determine the domain display name for Oracle Content DB.	If you have multiple Oracle Content DB databases registered with Oracle Internet Directory, you may be unsure of the value for the domain display name.	If you have only one Oracle Content DB database registered with Oracle Internet Directory, then the Oracle Content DB domain display name is **Content**.
		If you have multiple Oracle Content DB databases registered with Oracle Internet Directory, you can use Oracle Directory Manager to determine the correct domain display name, as follows:
		1. Open Oracle Directory Manager and connect to Oracle Internet Directory as the `cn=orcladmin` user.
		2. Under Entry Management, navigate through the tree to the following entry:
		`cn=IFS,cn=Products,cn=OracleContext`
		3. Under this entry, there are mutliple entries of the following format:
		`orclApplicationCommonName=domain_display_name`
		4. Select each entry and note the value of the `seealso` property, which appears in the following format:
		`orclReferenceName=database_service_name,cn=DatabaseInstances,cn=IFS,cn=Products,cn=OracleContext`
		The `orclApplicationCommonName` entry whose `seealso` property includes the service name of your database is the entry that shows the correct domain display name.
		Alternatively, you can find the domain display name using the following `ldapsearch` command on the OracleAS Infrastructure computer:
		`$ORACLE_HOME/bin/ldapsearch -h fully_qualified_infra_host_name -p Oracle_Internet_Directory_Port -D cn=orcladmin -w password_for_cn=orcladmin_user -b "cn=IFS,cn=Products,cn=OracleContext" -s one "objectclass=orclApplicationEntity" seealso`
		For example:
		`$ORACLE_HOME/bin/ldapsearch -h infrahost.company.com -p 389 -D cn=orcladmin -w mypassword -b "cn=IFS,cn=Products,cn=OracleContext" -s one "objectclass=orclApplicationEntity" seealso`
		This command will return one result for each Oracle Content DB repository registered with Oracle Internet Directory. These results will appear similar to the following:
		`orclApplicationCommonName=domain_display_name,cn=IFS,cn=Products,cn=OracleContext`
		
		`seealso=orclreferencename=database_service_name,cn=DatabaseInstances,cn=IFS,cn=Products,cn=OracleContext`
		The domain display name for your Oracle Content DB instance is the domain display name with a `seealso` value that includes the service name for your database.

The administrator has uploaded files and removed them, and does not see the space retrieved in the tablespace.	The Initial Time of Day and Activation Period has been set incorrectly for the `Content GarbageCollectionAgent`.	Use the Application Server Control to view the Initial Time of Day and Activation Period entries for the Content Garbage Collection Agent. Also check the node log and see if the Content Garbage Collection Agent is being activated at periodic intervals.

Table A–1 (Cont.) General Administration Issues

Problem	Probable Cause	Corrective Action
On UNIX systems, the regular node does not respond to `opmnctl stop` or `opmnctl restart` commands.	The node is hanging and must be stopped manually by the root user.	Because regular nodes run as root, nodes that are hanging must be shut down manually by the root user: `kill -9 process-id` To find out whether a node is hanging, use the `opmnctl status` command. Nodes that are hanging will show a status of "Stop." Nodes sometimes hang when the middle tier computer is low on resources, causing the node startup time to exceed 5 minutes.
Cannot log in to a new Site that was added using the Application Server Control.	`OC4J_Content` was not restarted after the Site was added.	You must restart `OC4J_Content` after you add a new Site. Restart `OC4J_Content` from the Content DB Home page in the Application Server Control, or use the following `opmnctl` command: `opmnctl restartproc process-type=OC4J_Content`
In the Application Server Control, the following error message appears for a particular server on the Node page: "This server is configured but not loaded now."	The server may not have been configured correctly, or the server may have an initialization or loading problem. This message also appears when the server has been deleted from the node at run time, but still exists in the node configuration.	Check the node log for information about possible initialization and loading errors for this server.

Solving Problems with Oracle Content DB Protocols

Table A–2 provides information about how to troubleshoot problems with Oracle Content DB protocols.

Table A–2 Protocol Issues

Problem	Probable Cause	Corrective Action
Problems with outbound FTP on UNIX.	You are using `/usr/bin/ftp` on UNIX and the default port number in `/etc/services` is a port other than 21, such as 2100.	Specify the port number explicitly, for example, `ftp ifs.us.oracle.com 21`, where 21 is the port assigned.
Cannot log in to FTP.	The FTP password has not been set.	Log in to Oracle Content DB with the user account that cannot access FTP and set an FTP password. You can then log in to FTP using the FTP password.
Multibyte file names for files that were uploaded over FTP appear garbled in the Web client.	Protocol command character set was not specified for the FTP client.	When uploading files with multibyte file names over FTP, you must specify a protocol command character set to ensure the file names are properly encoded. This step is only required when the installation locale has a different default character set than the file name you are specifying over FTP. For example, if you want to upload a file with a Japanese file name over FTP, but the installation locale is Spanish, explicitly set the protocol command character set to shift_jis, as follows: `FTP> quote setcommandcharacterset shift_jis` See "Globalization and the Oracle Content DB Protocols" on page G-3 for more information about protocol command character sets.

Solving Performance Problems

Table A–3 provides information about how to troubleshoot problems with Oracle Content DB performance.

Table A–3 Performance Issues

Problem	Probable Cause	Corrective Action
Server is generally slow for read and write activity (case #1).	Server memory is overcommitted. The server is excessively swapping memory blocks to disk.	Run system monitoring tools, such as `vmstat` (UNIX) and look for excessive page swapping to verify the problem. Adjust the following parameters in the `init.ora` file for the database: ▪ Reduce `processes`. ▪ Reduce `open_cursors`. ▪ Reduce `db_block_buffers`. Stop unneeded Java VMs or other unneeded processes. You may also need to add memory to your server or, if you are running a single-tier configuration, reconfigure your Oracle Content DB server into a two-tier configuration. For more information about adjusting the parameters in the `init.ora` file, see *Oracle Content Database Installation Guide* for your platform.
Server is generally slow for read and write activity (case #2).	`CTXHX` is using 100 percent of your CPU.	See Appendix C, "Managing the Oracle Text Index".
Server is slow only on read or search activity.	Large volumes of data have been loaded but the CBO statistics were not updated.	If the Cost-Based Optimizer is using out-of-date statistics data, performance suffers. Run the `analyze.sql` script located in the *`ORACLE_HOME`*`/content/admin/sql` directory to refresh the statistics.
Server is slow only on content-based search activity (case #1).	Oracle Text tablespaces are on the same disk as other database files.	Move the Oracle Text tablespaces to other disks. See *Oracle Database Administrator's Guide* for more information about moving tablespaces.
Server is slow only on content-based search activity (case #2).	Oracle Text indexes have become fragmented.	Regularly optimize the Oracle Text Oracle index `IFS_TEXT`. See "Maintaining the IFS_TEXT Index by Using the Oracle Text PL/SQL Packages" on page C-2 for more information.
Server is slow only on write activity (case #1).	Large amounts of documents are being loaded and the Redo logs are too small.	Add two or more 100 MB or larger Redo logs. See *Oracle Database Administrator's Guide* for more information. In general, Redo logs should be switching every hour or less frequently. See the *`ORACLE_HOME`*`/rdbms/sid/bdump` directory for the latest logs which indicate the frequency of Redo log switching.
Server is slow only on write activity (case #2).	Large amounts of documents are being loaded and the Redo logs are on the same disk as the database files.	Place the Redo logs on a separate disk from the database files. See *Oracle Database Administrator's Guide* and *Oracle Database Performance Tuning Guide* for more information. For optimal performance, dedicate one or more disks (and, if possible, a disk controller) exclusively to the Redo logs, and optimize the disks for sequential write activity. For example, on Solaris Operating System (SPARC), you may choose raw partitions or UNIX file systems for the disks. If you choose UNIX file systems on Solaris 2.6 or later, use the "forcedirection" option when mounting the file systems. These options should only be used if the file systems are dedicated exclusively to the Redo logs.

B

Migrating Content to Oracle Content DB

This chapter provides information about how to migrate content and users from legacy systems to Oracle Content DB. Oracle Content DB migration is applicable to customers migrating from the following systems:

- Oracle Content Management SDK
- Third-party applications, such as Novell

Oracle Content DB does not currently offer a migration toolkit. You must migrate your files manually. If you are migrating a very large number of files and require assistance, contact Oracle Support Services.

This appendix provides information about the following topics:

- Migration Tasks
- Migrating Oracle Content DB Users
- Creating Oracle Content DB Libraries
- Migrating Oracle Content DB Content

Migration Tasks

Consolidating users, folder hierarchy, content, and access privileges from other file server systems to Oracle Content DB involves the following tasks:

- Migrating Oracle Content DB Users: You need to move the user list from the old file system to the new one. In other words, you need to re-create each user in Oracle Content DB, by creating users in Oracle Internet Directory.
- Creating Oracle Content DB Libraries: If you have folders grouped into logical structures with specific security, you can create corresponding Libraries in Oracle Content DB with the same membership and access permissions.
- Migrating Oracle Content DB Content: You must copy the actual files and folders from the old system to the new one.

Migrating Oracle Content DB Users

The first task in moving to a new Oracle Content DB server is creating the user list.

For each user you want to migrate to Oracle Content DB, create a user in Oracle Internet Directory. See *Oracle Internet Directory Administrator's Guide* for more information.

After users have been created in Oracle Internet Directory, they are automatically provisioned in Oracle Content DB by the Oracle Internet Directory Credential Manager Agent. Also, once a user has been created in Oracle Internet Directory, signing on to Oracle Content DB as that user immediately provisions the user in Oracle Content DB.

Creating Oracle Content DB Libraries

To migrate user groups into Oracle Content DB, you must create or update corresponding Libraries and member roles in Oracle Content DB.

Scripted Library Creation

If your management tools let you export group information to a file, you can write a translation script to convert the groups into XML format. Then, you can use the Library Creation tool to create corresponding Libraries in Oracle Content DB. See the developer documentation for more information about the Library Creation tool.

Migrating Oracle Content DB Content

After creating users and Libraries, the next step is to move files and folders into Oracle Content DB. However, if your old file system had application-specific metadata, this information cannot be automatically copied.

How to Copy the Data

Use one of the following methods to copy your files:

- **File Transfer Protocol (FTP or FTPS):** FTP is the most lightweight protocol and can move large amount of data faster than other protocols. For bulk operations, such as migrating from an existing system, FTP is the preferred protocol. You need to use either a command-line FTP application or a Graphical User Interface (GUI) FTP client for this. As an alternative, you can use FTPS. FTPS is FTP with the added option of Secure Socket Layer (SSL) security. See "Using FTP with Oracle Content DB" on page 4-2 for information about how to enable and use FTP or FTPS.
- **Web-based Distributed Authoring and Versioning (WebDAV):** WebDAV, a protocol designed for Internet and intranet collaboration on files, enables you to drag and drop data from one system to another. If you want to retain the file structure, click and drag the entire directory structure from the original file system into Oracle Content DB, or drag different parts of the directory tree separately, confirming that each part of the tree has been copied before copying the next one.

  See "Using WebDAV with Oracle Content DB" on page 4-6 for more information about using WebDAV.
- **Oracle Drive:** Oracle Drive is a desktop client that uses the WebDAV protocol to access Oracle Content DB. After it is installed, Oracle Drive appears as a mapped drive in your Windows Explorer. Oracle Drive also provides file synchronization capabilities between your local computer and Oracle Content DB. See "Using Oracle Drive with Oracle Content DB" on page 4-7 for more information.

C

Managing the Oracle Text Index

Oracle Content DB uses Oracle Text to facilitate full-text search and other advanced capabilities. The speed with which results are returned depends on several factors, including the quality of the Oracle Text index used with Oracle Content DB (`IFS_TEXT`). The performance of the search can also depend on how much time you let elapse before a search times out.

Oracle Content DB uses an additional index, the `IFS_LYKE` index, to speed up substring searches on known items. For example, the `IFS_LYKE` index facilitates searches such as "*planning*" or "*.doc." The `IFS_LYKE` index is automatically created and maintained and does not normally require any administration. If you are having problems related to the `IFS_LYKE` index, contact Oracle Support Services for troubleshooting information.

This appendix provides information about how to maintain the Oracle Text index to ensure optimal Oracle Content DB performance, and includes these topics:

- Oracle Text Tablespaces and Disk Utilization
- Creating and Maintaining the Oracle Text Index
- Modifying the Search Timeout Parameter
- Troubleshooting Oracle Text Problems

Previous names for Oracle Text include Oracle Context and Oracle *inter*Media Text. Many of the underlying indexes, views, tables, and various PL/SQL packages referred to in much of the administrator and application developer documentation still use Context or *inter*Media-related terminology.

For detailed information about Oracle Text, visit the Oracle Technology Network at `http://www.oracle.com/technology/products/text/`.

Oracle Text Tablespaces and Disk Utilization

Disk space for Oracle Text is divided among three distinct tablespaces:

- The **Oracle Text Tokens** tablespace (`CONTENT_IFS_CTX_I`) contains tables that hold text tokens (separate words) that exist within the various indexed documents. The storage for these text tokens is roughly proportional to the ASCII content of the document. The ASCII content percentage will vary depending on the format of the original document. Text files only have white space as their non-ASCII content and, therefore, will incur a greater per-document percentage overhead. Document types such as Microsoft Word or PowerPoint contain large amounts of data required for formatting that does not qualify as text tokens. The per-document percentage on these types of documents will, therefore, be lower.

On a system with diverse content types, the expected overhead is approximately 8 percent of the sum of the original sizes of the indexed documents.

- The **Oracle Text Index** tablespace (`CONTENT_IFS_CTX_X`) contains the B*tree database index that is used against the text token information stored in the Oracle Text Tokens tablespace. This will grow as a function of the ASCII content, just as the Oracle Text Tokens tablespace does. On a system with diverse content types, the expected overhead is approximately 4 percent of the sum of the ASCII content of the documents, or approximately 1 percent of the sum of the total sizes of the indexed documents.
- The **Oracle Text Other** tablespace (`CONTENT_IFS_CTX_K`) contains the tables and indexes required to translate from the Oracle Content DB locator of a document (the Oracle Content DB DocID) to the Oracle Text locator of that same document (the Oracle Text DocID). The expected space utilization for this tablespace is approximately 70 bytes for each indexed document.

Use this information to estimate and plan disk storage needs for your Oracle Content DB instance.

Creating and Maintaining the Oracle Text Index

The configuration process for Oracle Content DB uses the SQL scripts shown in Table C–1 to create and populate the `IFS_TEXT` index.

These scripts are located in the following directory:

ORACLE_HOME`/content/admin/sql`

Table C–1 SQL Scripts for Creating Oracle Text Index

Script	Usage	Log In As	Arguments
`CreateContextFunnelProcedure.sql`	Creates the procedure used by USER_DATASTORE.	*content_db_schema_owner* (typically `CONTENT`)	None
`GrantContextToIFS.sql`	Grants the Oracle Content DB user (schema) privileges on the Oracle Text-specific commands required to maintain the index.	*sys*	*content_db_schema_name* (typically `CONTENT`)
`CreateContextPreferences.sql`	Tablespace and other text preferences are created by the Oracle Content DB user.	*content_db_schema_owner* (typically `CONTENT`)	*OracleText_index_tablespace* *OracleText_keymap_tablespace* *OracleText_data_tablespace* *content_db_schema_name* (typically `CONTENT`)
`CreateContextIndex.sql`	Creates the `IFS_TEXT` index based on the text preferences.	*content_db_schema_owner* (typically `CONTENT`)	None

Maintaining the IFS_TEXT Index by Using the Oracle Text PL/SQL Packages

Two PL/SQL procedures are provided with Oracle Text for maintaining the index. Unlike a regular database index, the Oracle Text index is not dynamically updated with each insert or update of information. Rather, the index must be refreshed (or synchronized) periodically, using the Oracle Text stored procedure `ctx_ddl.sync_index`.

The `ctx_ddl.sync_index` procedure does not rebuild the entire index; it adds and deletes records that have changed since the last synchronization. Because the changes are incremental, the more frequently this procedure is run, the faster it runs. Over the course of time, however, the index can become fragmented, so a companion procedure (`ctx_ddl.optimize_index`) is provided to optimize the index.

During Oracle Content DB configuration, the procedures to synchronize and optimize the `IFS_TEXT` index are automatically set up to run periodically in the background, using the `DBMS_JOBS` package of Oracle Database. `DBMS_JOBS` procedures, which are similar to `cron jobs` on UNIX systems, are portable across all platforms on which Oracle Database runs.

When the Oracle Content DB schema is created during configuration, two `DBMS_JOBS` are set up: Sync Job and Optimize Job. The name of the Oracle Content DB schema is typically `CONTENT`.

Note: Sync Job and Optimize Job are only created automatically when a new schema is created. If you are upgrading from an existing schema, these jobs will not be created for you.

Sync Job

Sync Job will periodically call the `ctx_ddl.sync_index()` method. This method indexes the documents that were created or updated since the last run. By default, this job runs every 30 minutes.

Optimize Job

Optimize Job will periodically call the `ctx_ddl.optimize_index()` method. The goal of this job is to optimize the `IFS_TEXT` index by defragmenting it. By default, this job is run in `FULL` mode, with a maximum of 1 hour allocated for the optimization task. The job runs every 24 hours, starting at midnight.

Monitoring DBMS_JOBS

`DBMS_JOB` logs can be found under the Oracle home that hosts Oracle Database, in the directory that holds the background process logs. This directory is pointed to by the `BACKGROUND_DUMP_DEST` configuration parameter of the database server. You can recognize the log trace files by their name pattern, `DBNAME_j###_`*`process-id`*`.trc`.

Another database configuration parameter, `JOB_QUEUE_PROCESSES`, determines how many processes are available to run all background tasks. You may need to increase the value of this parameter if not enough processes are available to run Sync Job and Optimize Job. The default value is 10.

You can also look at the `USER_JOBS` view to see a list of all the jobs set up by the current schema user. The `USER_JOBS` view shows details such as the PL/SQL being run by each job, the last time each job was run, and when the jobs are scheduled to be run next. To see the `USER_JOBS` view, log on to the Oracle Content DB schema (typically `CONTENT`) using SQL*Plus.

Changing or Removing the Default DBMS_JOBS

Two SQL files are used to set up and clear the `DBMS_JOBS` in Oracle Content DB: `SetupContextJobs.sql` and `ClearContextJobs.sql`. These files are located in the following directory:

```
ORACLE_HOME/content/admin/sql
```

`SetupContextJobs.sql` is used by the system during configuration to set up Sync Job and Optimize Job. `ClearContextJobs.sql` is provided to remove Sync Job and Optimize Job, in case you want to set up your own `DBMS_JOBS`.

See *Oracle Database Administrator's Guide* for information about setting up your own `DBMS_JOBS`. You can also look at Sync Job and Optimize Job as examples.

Manually Synchronizing and Optimizing IFS_TEXT

To synchronize an existing `IFS_TEXT` index, use SQL*Plus to connect as the Oracle Content DB schema user (typically `CONTENT`), and enter:

```
exec ctx_ddl.sync_index('ifs_text');
```

You can also run the `SyncContextIndex.sql` script from the *`ORACLE_HOME`*`/content/admin/sql` directory. In addition to synchronizing the `IFS_TEXT` index, this script will display extra log information on the console.

To optimize an existing `IFS_TEXT` index, use SQL*Plus to connect as the Oracle Content DB schema user (typically `CONTENT`), and enter:

```
exec ctx_ddl.optimize_index('ifs_text', 'FAST');
```

or

```
exec ctx_ddl.optimize_index('ifs_text', 'FULL', maxtime);
```

Monitoring Oracle Text Indexing of Oracle Content DB Documents

Oracle Content DB provides some utility-type SQL scripts to facilitate interaction with Oracle Text. Read each `.sql` file for additional usage details. All scripts are available in:

```
ORACLE_HOME/content/admin/sql
```

Table C–2 lists the SQL scripts provided by Oracle Content DB to monitor Oracle Text.

Table C–2 SQL Scripts for Monitoring Oracle Text Indexing

Script	Usage
`ViewContextErrors.sql`	Script that decodes the operating system-specific errors that were generated during Oracle Text indexing.
`SyncContextIndex.sql`	Script that synchronizes the Oracle Text index and enables you to monitor the Oracle Text synchronization process. Uncomment the first two lines in the script, which includes a call to `ctx_output.add_event()`, to monitor on a row ID by row ID basis.
`ViewDocumentByRowID.sql`	Script that enables you to view additional information about a document that is indexed by Oracle Text. Use the `docid` from the Oracle Text log with this script.

Indexing Non-Standard Content Types

Oracle Content DB does, not by default, index every file that is moved into the system, but you can configure it to index any type of content you choose. To do this, designate the MIME type as Indexed on the New Format page (or Edit Format page, if the format already exists) in the Application Server Control. The MIME type of a document is determined by its extension.

For example, you may want to index all your C# (`.cs`) source code files. To do so:

1. Use the Application Server Control to add the `.cs` MIME type, and designate it as **Indexed** on the New Format page.
2. Upload the files into the repository.
3. Synchronize the index using the procedure discussed in "Manually Synchronizing and Optimizing IFS_TEXT" on page C-4.

See "Default Formats" on page 10-3 for a list of formats that are indexed by default in Oracle Content DB.

Modifying the Search Timeout Parameter

The `IFS.SERVICE.SESSION.DefaultSearchTimeoutPeriod` service configuration parameter specifies the timeout period for a running search that has not yet returned results. The default setting for this parameter (in the default service configurations) is 60 seconds. If you increase this value, users will wait longer than a minute before a search times out; decrease the value to shorten the time in which a running search will time out.

See "Modifying Service Configurations" on page 8-16 for information about how to modify service configuration parameters.

Troubleshooting Oracle Text Problems

Table C–3 provides Oracle Text troubleshooting information.

Table C–3 Troubleshooting Oracle Text Problems

Problem	Probable Cause	Corrective Action
Cannot search on contents of any documents.	Documents have not been indexed.	Start the database instance and ensure that the Oracle Text indexing jobs are running. See "Creating and Maintaining the Oracle Text Index" on page C-2 for more information.
Server is slow only on content-based search activity (case #1).	Oracle Text tablespaces are on the same disk as other database files.	Move the Oracle Text tablespaces to other disks. See *Oracle Database Administrator's Guide* for more information about moving tablespaces.
Server is slow only on content-based search activity (case #2).	Oracle Text indexes have become fragmented.	Regularly optimize the Oracle Text index `GLOBALINDEXEDBLOB_I`. See "Manually Synchronizing and Optimizing IFS_TEXT" on page C-4 for more information.

Table C–3 (Cont.) Troubleshooting Oracle Text Problems

Problem	Probable Cause	Corrective Action
Searching on the contents of new documents stops working.	A recent document has caused Oracle Text server to fail.	**1.** Log in to SQL*Plus as *`content_db_schema`*/*`schema_password`*, and enter the following command: `select count(*) from ctx_user_pending;` The name of the Oracle Content DB schema is typically `CONTENT`. **2.** If there are any rows in that view and the rows are not changing, then a recent document has caused Oracle Text to stop indexing. To determine which Oracle Content DB documents these rows refer to, see the problem "Oracle Content DB rows show up in the Oracle Text view `ctx_user_index_errors`." **3.** Check again to see if there are any rows in `ctx_user_pending` and, if so, that the rows are changing. **4.** If this does not resolve the issue, contact your Oracle Support Services representative for further assistance.

Oracle Content DB rows show up in the Oracle Text view `ctx_user_index_errors`.	Oracle Content DB documents are corrupt or do not have the correct extension.	**1.** Determine which Oracle Content DB document is being referred to, based on the `err_texkey` from `ctx_user_index_errors`.
		`sqlplus` *`content_db_schema`*/*`schema_password`*
		
		`select du.uniquename, vd.name, co.contentsize,`
		`cs.id, vd.id`
		`from odmv_document vd, odm_contentobject co,`
		`odmm_contentstore cs, odm_document od,`
		`odm_directoryuser du`
		`where vd.id = od.id`
		`and od.contentobject = co.id`
		`and co.content = cs.id`
		`and du.id = vd.owner`
		`and cs.id in`
		`(`
		`select distinct od.id`
		`from ctx_user_index_errors cp, odmm_contentstore od`
		`where od.rowid =` **`err_textkey`**
		`)`
		`order by cs.id;`
		2. Log in to Oracle Content DB as a user with the Content Administrator role (such as the `orcladmin` user) and switch to Administration Mode.
		3. Search on the document name *`vd.id`*, where *`vd.id`* is the `vd.id` returned from the `SELECT` statement provided in Step 1.
		4. Check document attributes, such as document size, to ensure that it is the correct document.
		5. Examine this document, and consider these questions:
		Is the file damaged in any way?
		Is the file name extension correct for this document?
		Is the character set of the document correct?
		6. If no obvious problems are found, send the document to your Oracle Support Services representative for further diagnosis.

Table C–3 (Cont.) Troubleshooting Oracle Text Problems

Problem	Probable Cause	Corrective Action
Oracle Content DB rows never get processed and never leave the Oracle Text view `ctx_user_pending`.	Oracle Content DB documents are corrupt or do not have the correct extension.	**1.** Follow the steps in "Oracle Content DB rows show up in the Oracle Text view `ctx_user_index_errors`." to determine which Oracle Content DB documents are being referred to, substituting `ctx_user_pending` for `ctx_user_index_errors` and `pnd_rowid` for `err_textkey`. **2.** Examine this document, and consider these questions: Is the file damaged in any way? Is the file name extension correct for this document? Is the character set of the document correct? **3.** If no obvious problems are found, send the document to your Oracle Support Services representative for further diagnosis. **4.** Delete the document from Oracle Content DB.

D

Service Configuration Properties

An Oracle Content DB service comprises a Java runtime environment for the protocol servers and agents that it supports. A service also manages connections to the database through JDBC. There are three default service configuration objects you can use to create new services on nodes:

- SmallServiceConfiguration
- MediumServiceConfiguration
- LargeServiceConfiguration

The differences among the three configuration templates are in the number of connections and sessions supported.

This appendix lists the service configuration properties and their default values.

Note: Do not use spaces to separate alternate values of a property. Instead, use a comma as a delimiter.

Table D–1 ***`IFS.SERVICE.*`*** ***Properties***

Property	Description and Usage Notes	Default	Required?
`IFS.SERVICE.CheckForOrphanSessionsPeriod`	Number of seconds between checks for orphan sessions. (Active sessions generate heartbeats. An orphan session is one that no longer generates session heartbeats. When the service detects an orphan session, it disconnects the session and releases the resources for the session.) Default is 60 seconds between checks. Set to 0 to disable the checking.	60	No
`IFS.SERVICE.DefaultCharacterSet`	This property is not used.	Not applicable	No
`IFS.SERVICE.DefaultLanguage`	This property is not used.	Not applicable	No
`IFS.SERVICE.LockTimeoutPeriod`	The time period (in seconds) for a session to wait when attempting to lock database resources when performing an update operation. If unable to lock the required database resources within the time period indicated, the update operation will time out, and an exception will occur.	10	No

Table D–1 (Cont.) `IFS.SERVICE.*` Properties

Property	**Description and Usage Notes**	**Default**	**Required?**
`IFS.SERVICE.MaximumConcurrentSessions`	Maximum number of Library **sessions** the service can support concurrently. Default of 0 means unlimited. This value determines how many Library sessions are available for outstanding user requests, across all users. It does not limit the number of users who can log in.	200 - Small 70 - Medium 40 - Large	No
`IFS.SERVICE.OrphanSessionTimeoutPeriod`	Number of seconds after which a session that no longer generates a heartbeat becomes an orphan. Set to 0 to disable orphan session timeout.	600	No
`IFS.SERVICE.PollForEventsFromOtherServicesPeriod`	Seconds between checks for incoming events from other services. Set to 0 to disable interservice event polling.	2	No
`IFS.SERVICE.ServiceKeepAliveEventPeriod`	Seconds between service heartbeats. The Service Watchdog Agent detects services that cease to have a heartbeat, and cleans up information associated with the failed service in the Oracle Content DB repository. Set to 0 to disable the heartbeat.	60	No
`IFS.SERVICE.SessionOperationTimeoutPeriod`	Number of seconds after which certain Oracle Content DB API calls are terminated, even if incomplete. If an operation times out in this manner, it is terminated, its transaction is terminated, and an exception occurs. The session performing the operation remains valid. Set to 0 to disable session operation timeout.	300	No
`IFS.SERVICE.TransportEventsToOtherServicesPeriod`	Maximum length of time (seconds) that outgoing events are buffered before sending. Set to 0 to disable outgoing event buffer.	2	No
`IFS.SERVICE.ACLCACHE.EmergencyTrigger`	The cache size, in ACLs, at which the service ACL cache performs an immediate purge of data that has not been recently used. Must be greater than `IFS.SERVICE.ACLCACHE.UrgentTrigger` but less than `IFS.SERVICE.ACLCACHE.Size`.	600 - Small 2400 - Medium 6000 - Large	No
`IFS.SERVICE.ACLCACHE.NormalTrigger`	The cache size, in ACLs, at which the service ACL cache schedules a low-priority purge of data that has not been recently used.	500 - Small 2000 - Medium 5000 - Large	No
`IFS.SERVICE.ACLCACHE.PurgeTarget`	The target cache size, in ACLs, on completion of a purge cycle. Must be less than `IFS.SERVICE.ACLCACHE.NormalTrigger`.	400 - Small 1600 - Medium 4000 - Large	No
`IFS.SERVICE.ACLCACHE.Size`	The absolute maximum size of the service's ACL cache, in ACLs. The service ACL cache holds resolved access levels of ACLs.	750 - Small 3000 - Medium 7500 - Large	No
`IFS.SERVICE.ACLCACHE.UrgentTrigger`	The cache size, in ACLs, at which the service ACL cache schedules a high-priority purge of data that has not been recently used. Must be greater than `IFS.SERVICE.ACLCACHE.NormalTrigger`.	550 - Small 2200 - Medium 5500 - Large	No

Table D–1 (Cont.) `IFS.SERVICE.*` Properties

Property	Description and Usage Notes	Default	Required?
`IFS.SERVICE.CONNECTIONPOOL.READONLY.MaximumSize`	The absolute maximum number of database connections in the read-only connection pool. Must be greater than or equal to `IFS.SERVICE.CONNECTIONPOOL.READONLY.TargetSize`.	20 - Small 20 - Medium 20 - Large	No
`IFS.SERVICE.CONNECTIONPOOL.READONLY.MaximumSizeTimeout`	The maximum period, in milliseconds, that a service will postpone a connection allocation request when there are no unallocated connections, if the current size of the read-only connection pool is equal to its maximum size. If a database connection does not become available within this period, the allocation request will fail and an exception will occur.	10000	No
`IFS.SERVICE.CONNECTIONPOOL.READONLY.MinimumSize`	The initial number of database connections in the read-only connection pool.	2 - Small 4 - Medium 6 - Large	No
`IFS.SERVICE.CONNECTIONPOOL.READONLY.StatementCacheSizeTrigger`	The cache size, in number of statements, at which the statement cache schedules a purge.	105	No
`IFS.SERVICE.CONNECTIONPOOL.READONLY.StatementCacheTarget`	The target cache size, in number of statements, for the statement cache upon completion of a purge cycle. Must be less than `IFS.SERVICE.CONNECTIONPOOL.READONLY.StatementCacheSizeTrigger`.	95	No
`IFS.SERVICE.CONNECTIONPOOL.READONLY.TargetSize`	The target maximum number of database connections in the read-only connection pool. Must be greater than or equal to `IFS.SERVICE.CONNECTIONPOOL.READONLY.MinimumSize`.	10 - Small 10 - Medium 15 - Large	No
`IFS.SERVICE.CONNECTIONPOOL.READONLY.TargetSizeTimeout`	The maximum period, in milliseconds, that the service will postpone a connection allocation request when there are no unallocated connections, if the current size of the read-only connection pool is greater than or equal to its target size, but less than the maximum size. If a database connection does not become available within this period, a new connection will be created.	1000	No
`IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSize`	The absolute maximum number of database connections in the writeable connection pool. Must be greater than or equal to `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSize`.	20 - Small 20 - Medium 20 - Large	No
`IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSizeTimeout`	The maximum period, in milliseconds, that a service will postpone a connection allocation request when there are no unallocated connections, if the current size of the writeable connection pool is equal to its maximum size. If a database connection does not become available within this period, the allocation request will fail and an exception will occur.	10000	No

Table D–1 (Cont.) ***`IFS.SERVICE.*`*** *Properties*

Property	Description and Usage Notes	Default	Required?
`IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MinimumSize`	The initial number of database connections in the writeable connection pool.	2 - Small 4 - Medium 6 - Large	No
`IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheSizeTrigger`	The cache size, in number of statements, at which the statement cache schedules a purge.	200	No
`IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheTarget`	The target cache size, in number of statements, for the statement cache upon completion of a purge cycle. Must be less than `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheSizeTrigger`.	160	No
`IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSize`	The target maximum number of database connections in the writeable connection pool. Must be greater than or equal to `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MinimumSize`.	10 - Small 10 - Medium 15 - Large	No
`IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSizeTimeout`	The maximum period, in milliseconds, that the service will postpone a connection allocation request when there are no unallocated connections, if the current size of the writeable connection pool is greater than or equal to its target size, but less than the maximum size. If a database connection does not become available within this period, a new connection will be created.	1000	No
`IFS.SERVICE.CaseSensitiveAuthentication`	Whether, in performing cleartext authentication, passwords are case-sensitive.	false	No
`IFS.SERVICE.CREDENTIALMANAGER.CredentialNameTokenizer`	The fully qualified classname of the `CredentialNameTokenizer`.	`oracle.ifs.common.IfsCredentialNameTokenizer`	No
`IFS.SERVICE.CREDENTIALMANAGER.*`	The configuration of credential managers for the service. Do not edit these properties directly, except for `IFS.SERVICE.CREDENTIALMANAGER.Oid.OidSsl` and `IFS.SERVICE.CREDENTIALMANAGER.Oid.OidUrl`.	Not applicable	Not applicable
`IFS.SERVICE.CREDENTIALMANAGER.Oid.OidSsl`	Whether Oracle Content DB connects to Oracle Internet Directory using SSL.	Set during configuration	No
`IFS.SERVICE.CREDENTIALMANAGER.Oid.OidUrl`	The URL for Oracle Internet Directory.	Set during configuration	No
`IFS.SERVICE.DATACACHE.Size`	The absolute maximum size of the service's data cache, in LibraryObjects. The service data cache holds the attribute values of recently used LibraryObjects.	7500 - Small 30000 - Medium 75000 - Large	No
`IFS.SERVICE.DATACACHE.NormalTrigger`	The cache size, in LibraryObjects, at which the service data cache schedules a low-priority purge of data that has not been recently used.	5000 - Small 20000 - Medium 50000 - Large	No

Table D–1 (Cont.) `IFS.SERVICE.*` Properties

Property	Description and Usage Notes	Default	Required?
`IFS.SERVICE.DATACACHE.UrgentTrigger`	The cache size, in LibraryObjects, at which the service data cache schedules a high-priority purge of data that has not been recently used. Must be greater than `IFS.SERVICE.DATACACHE.NormalTrigger`.	5500 - Small 22000 - Medium 55000 - Large	No
`IFS.SERVICE.DATACACHE.EmergencyTrigger`	The cache size, in LibraryObjects, at which the service data cache performs an immediate purge of data that has not been recently used. Must be greater than `IFS.SERVICE.DATACACHE.UrgentTrigger` but less than `IFS.SERVICE.DATACACHE.Size`.	6000 - Small 24000 - Medium 60000 - Large	No
`IFS.SERVICE.DATACACHE.PurgeTarget`	The target cache size, in LibraryObjects, on completion of a purge cycle. Must be less than `IFS.SERVICE.DATACACHE.NormalTrigger`.	4000 - Small 16000 - Medium 40000 - Large	No
`IFS.SERVICE.HSM.PrimaryDevice`	This property is not used.	Not applicable	Not applicable
`IFS.SERVICE.JDBC.DefaultRowPrefetch`	Number of result set rows prefetched. If set to null or 0, prefetches 10 rows. Do not change.	0	No
`IFS.SERVICE.JDBC.DriverType`	Specifies the JDBC driver type. Do not change.	oci8	No
`IFS.SERVICE.JDBC.TracingEnabled`	Sends JDBC debugging information to the standard output. Do not change.	false	No
`IFS.SERVICE.SESSION.TransactionStackSize`	The maximum number of nested transactions by the session.	100	No
`IFS.SERVICE.SESSION.EventPoller`	The event poller used by a session to generate the heartbeat of the session. Must be either `oracle.ifs.beans.LibrarySessionEventPollerThreadPerProcess` (recommended) or `oracle.ifs.beans.LibrarySessionEventPollerThreadPerSession`.	`oracle.ifs.beans.LibrarySessionEventPollerThreadPerProcess`	No
`IFS.SERVICE.SESSION.EventPollerPeriod`	The period, in milliseconds, of the session's heartbeat. In addition to indicating the health of the session to the service, the heartbeat allows an idle session to process events generated by other sessions or services.	2500	No
`IFS.SERVICE.SESSION.DefaultSearchTimeoutPeriod`	The period, in seconds, after which a search API call is terminated, even if incomplete. If a search times out in this manner, it is terminated and an exception occurs. The session performing the search remains valid. A value of 0 disables search timeouts.	60	No
`IFS.SERVICE.SESSION.BEANSOBJECTCACHE.Size`	The target maximum size of the bean-side session object cache, in LibraryObjects. The bean-side session object cache holds instances of `oracle.ifs.beans.LibraryObject`. If `IFS.SERVICE.SESSION.SERVEROBJECTCACHE.IsUnbounded` is false, this value is ignored and implicitly equal to `IFS.SERVICE.SESSION.SERVEROBJECTCACHE.Size`.	750	No
`IFS.SERVICE.SESSION.FOLDERPATHCACHE.Enabled`	Whether the session caches the resolution of folder paths.	true	No

Table D–1 (Cont.) `IFS.SERVICE.*` Properties

Property	Description and Usage Notes	Default	Required?
`IFS.SERVICE.SESSION.FOLDERPATHCACHE.Size`	The absolute maximum size of the folder path cache of the session, in cached folder paths.	150	No
`IFS.SERVICE.SESSION.FOLDERPATHCACHE.NormalTrigger`	The cache size, in folder paths, at which the session's folder path cache schedules a low-priority purge of data that has not been recently used.	100	No
`IFS.SERVICE.SESSION.FOLDERPATHCACHE.UrgentTrigger`	The cache size, in folder paths, at which the folder path cache of the session schedules a high-priority purge of data that has not been recently used. Must be greater than `IFS.SERVICE.SESSION.FOLDERPATHCACHE.NormalTrigger` and less than `IFS.SERVICE.SESSION.FOLDERPATHCACHE.Size`.	110	No
`IFS.SERVICE.SESSION.FOLDERPATHCACHE.PurgeTarget`	The target cache size, in folder paths, on completion of a purge cycle. Must be less than `IFS.SERVICE.SESSION.FOLDERPATHCACHE.NormalTrigger`.	80	No
`IFS.SERVICE.SESSION.SERVEROBJECTCACHE.Size`	The absolute maximum size of the server-side session object cache, in LibraryObjects. The server-side session object cache holds instances of `oracle.ifs.server.S_LibraryObject` and `oracle.ifs.beans.LibraryObject`.	750	No
`IFS.SERVICE.SESSION.SERVEROBJECTCACHE.NormalTrigger`	The cache size, in LibraryObjects, at which the session data caches schedule a low-priority purge of data that has not been recently used.	500	No
`IFS.SERVICE.SESSION.SERVEROBJECTCACHE.UrgentTrigger`	The cache size, in LibraryObjects, at which the session data caches schedule a high-priority purge of data that has not been recently used. Must be greater than `IFS.SERVICE.SESSION.SERVEROBJECTCACHE.NormalTrigger`.	550	No
`IFS.SERVICE.SESSION.SERVEROBJECTCACHE.EmergencyTrigger`	The cache size, in LibraryObjects, at which the session data caches perform an immediate purge of data that has not been recently used. Must be greater than `IFS.SERVICE.SESSION.SERVEROBJECTCACHE.UrgentTrigger` but less than `IFS.SERVICE.SESSION.SERVEROBJECTCACHE.Size`.	600	No
`IFS.SERVICE.SESSION.SERVEROBJECTCACHE.PurgeTarget`	The target cache size, in LibraryObjects, on completion of a purge cycle. Must be less than `IFS.SERVICE.SESSION.SERVEROBJECTCACHE.NormalTrigger`.	400	No
`IFS.SERVICE.TRACING.ChannelCount`	The number of trace logger channels. Oracle reserves channels 0 to `TraceLogger.LAST_RESERVED_CHANNEL`. See the Javadoc for class `oracle.ifs.common.TraceLogger` for a list of Oracle-defined channels.	50	No

Table D–1 (Cont.) `IFS.SERVICE.*` Properties

Property	Description and Usage Notes	Default	Required?
`IFS.SERVICE.TRACING.ServiceTraceType`	The destination of trace data generated by a service. Must be `TRACETYPE_NONE` (disabled) or `TRACETYPE_LOCAL` (writes to a file on the local file system).	`TRACETYPE_NONE`	No
`IFS.SERVICE.TRACING.ServerSessionTraceType`	The destination of trace data generated by a server-side session. Must be `TRACETYPE_NONE` (disabled), `TRACETYPE_LOCAL` (writes to a file on the local file system), `TRACETYPE_REMOTE` (routes to the service's trace logger), or `TRACETYPE_BOTH` (writes to a file on the local file system and routes to the service's trace logger).	`TRACETYPE_NONE`	No
`IFS.SERVICE.TRACING.BeansSessionTraceType`	The destination of trace data generated by a bean-side session. Must be `TRACETYPE_NONE` (disabled), `TRACETYPE_LOCAL` (writes to a file on the local file system), `TRACETYPE_REMOTE` (routes to the server-side session's trace logger), or `TRACETYPE_BOTH` (writes to a file on the local file system and routes to the server-side session's trace logger).	`TRACETYPE_NONE`	No
`IFS.SERVICE.TRACING.TraceLevelChanneln`	Tracing verbosity for trace channel *n*. Refer to the Javadoc for class `oracle.ifs.common.TraceLogger` for a list of Oracle-defined trace levels.	None	No
`IFS.SERVICE.TRACING.DefaultTraceLevel`	Default tracing verbosity for all trace channels. See `oracle.ifs.common.TraceLogger` Javadoc for a list of trace levels.	None	No

E

Server Configuration Properties

Each Oracle Content DB node can support multiple **servers**. These servers can be either protocol servers or agents:

- The protocol servers, such as the FTP server, listen for requests from clients on a specific Internet Protocol (IP) port and respond to requests according to the rules of the protocol specification.
- Agents perform operations periodically (time-based) or in response to events generated by other Oracle Content DB servers or processes (event-based). Although different agents can run in different nodes, each agent must run only on a single node. Typically, most of the agents that come with the software must be run to ensure a stable system.

Each server is based on a particular **server configuration** that holds the default values used when the server is started for an Oracle Content DB node. For example, a server configuration for the Oracle Content DB FTP server contains properties that specify the FTP port number, whether anonymous FTP connections are allowed, and the connection timeout period.

The properties listed in this appendix are all required for a protocol server or agent to run properly. When you install and configure an Oracle Content DB instance, the properties are configured using the default values shown in this appendix.

This appendix provides information about the following topics:

- FTP Server
- FTPS Server - Explicit
- FTPS Server - Implicit
- Garbage Collection Agent
- HTTP Server
- Inbound Queue Listener Agent
- Lock Expiration Agent
- Most Recent Doc Agent
- Oracle Event Handler Agent
- Oracle Internet Directory Credential Manager Agent
- Quota Agent
- Read Document Agent
- Reassign Quota Agent
- Records DB HTTP Server
- Records DB Lifecycle Agent
- Refresh Security Agent
- Secure Enterprise Search Group Agent
- Service Warmup Agent
- Service Watchdog Agent
- Statistics Agent
- Version Purge Agent
- Virus Repair Agent

Shared Properties

Table E–1 defines server configuration properties that are shared among more than one server or agent.

Table E–1 Shared Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.Class`	The class used to instantiate the server.	Default varies from server to server.
`IFS.SERVER.SESSION.LOCALE.Country`	Default country to be used in session localizer.	US
`IFS.SERVER.SESSION.LOCALE.Language`	Default language to be used in session localizer.	en
`IFS.SERVER.SESSION.User`	User name for server session. Must be a user with Oracle Content DB administrator privileges.	system

Table E–1 (Cont.) Shared Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.TIMER.ActivationPeriod`	Time interval for when the agent runs again. Specified as a number followed by a time unit, such as 4h to indicate a 4-hour interval. Time units are: h=hours, m=minutes, s=seconds	Default varies from server to server.
`IFS.SERVER.TIMER.InitialDelay`	The delay before the first time interval, relative to when the server is started. This property is ignored if a value is specified for `IFS.SERVER.TIMER.InitialTimeOfDay`.	Default varies from server to server.
`IFS.SERVER.TIMER.InitialTimeOfDay`	The first timer event. Set time based on a 24-hour clock.	00:15:00

Audit Event Dispatch Agent

The Audit Event Dispatch Agent is a time-based agent that dispatches raw audit events to other audit histories. This agent polls for new raw audit events, and copies them to all registered audit histories through registered AuditSpecification instances.

The default name for this server configuration is:

`AuditEventDispatchAgentConfiguration`

Table E–2 lists the properties for the Audit Event Dispatch Agent.

Table E–2 Audit Event Dispatch Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.AUDITEVENTDISPATCHAGENT.EventBatchSize`	The maximum number of events processed in a single iteration of this agent.	5000
`ECM.AGENT.AUDITEVENTDISPATCHAGENT.EventCountPublishingPeriod`	The number of activation periods that will elapse before the updated event counts are published. For example, if this property is set to 20, and `IFS.SERVER.TIMER.ActivationPeriod` is set to 3 seconds, then the event counts are updated every 1 minute.	20

Audit Event Handler Agent

This agent is not used.

Background Request Agent

The Background Request Agent is an event-based agent that reacts to requests placed by users for operations that take a long time to perform, such as modifying the Sharing properties of a Site. The agent asynchronously performs the requested operations to avoid performance problems.

The default name for this server configuration is:

`BackgroundRequestAgentConfiguration`

Table E–3 lists the properties for the Background Request Agent.

Table E–3 Background Request Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.BACKGROUNDREQUESTAGENT.EventBatchSize`	The maximum number of events processed in a single iteration of this agent.	5000

Cleanup Agent

The Cleanup Agent performs a variety of cleaning tasks on a periodic basis, such as deleting content in the Archive that has passed the expiration period set by the Content Administrator. Each of these tasks has a corresponding property called an Activation Multiplier that controls how often the task is performed.

The Activation Multiplier works in conjunction with the `IFS.SERVER.TIMER.ActivationPeriod` property. For example, if `IFS.SERVER.TIMER.ActivationPeriod` is set to 1h, and `ECM.AGENT.CLEANUPAGENT.EMPTYARCHIVE.ActivationMultiplier` is set to 8, then the Cleanup Agent will delete expired content in the Archive every 8 hours.

The descriptions and notes provided in Table E–4 assume an ActivationPeriod of 1 hour, which is the default for this agent.

The default name for this server configuration is:

```
CleanupAgentConfiguration
```

Table E–4 Cleanup Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.CLEANUPAGENT.ARCHIVETOBFILE.ActivationMultiplier`	Controls how often content in the Archive is moved to a BFILE. This action is only performed when BFILE archiving has been enabled. See "Setting Up Data Archiving" on page 5-7 for more information.	24
`ECM.AGENT.CLEANUPAGENT.BaseTimeOfDay`	The time of day from which all intervals for this agent are based. This property determines the time at which tasks will be run that perform only once every 24 hours, and the relative time for tasks performed only a few times in a 24-hour period. For example, if a task has an ActivationMultiplier of 8 and the BaseTimeOfDay is set to 20:15:00, that task will run at 20:15, 4:15, and 12:15.	20:15:00
`ECM.AGENT.CLEANUPAGENT.CALCULATEARCHIVEQUOTA.ActivationMultiplier`	Controls how often the quota used by files in the Archive for each Site is recalculated.	4
`ECM.AGENT.CLEANUPAGENT.CALCULATEDOMAINQUOTA.ActivationMultiplier`	Controls how often the total quota used by all files located in Libraries for each Site is recalculated.	1
`ECM.AGENT.CLEANUPAGENT.CLEARLINKREFERENCE.ActivationMultiplier`	Controls how often links that reference inaccessible items have their internal representation optimized.	12
`ECM.AGENT.CLEANUPAGENT.DELETEDOMAINADMINUSER.ActivationMultiplier`	Controls how often the administration mode representation for users is removed from the system, for users whose application administration access has been disabled for a sufficient period of time. This time period is controlled by the `ECM.AGENT.CLEANUPAGENT.DELETEDOMAINADMINUSER.InactivityPeriod` property.	12
`ECM.AGENT.CLEANUPAGENT.DELETEDOMAINADMINUSER.InactivityPeriod`	The amount of time the administration representation for a user remains after the user loses all application administration rights, before that user is removed from the system.	24h
`ECM.AGENT.CLEANUPAGENT.DELETEGRANT.ActivationMultiplier`	Controls how often security configurations are optimized to reflect users or groups that have been removed from the system.	24
`ECM.AGENT.CLEANUPAGENT.DELETETRASHACL.ActivationMultiplier`	Controls how often unused security configurations for items in Trash folders are removed from the system.	24

Table E–4 (Cont.) Cleanup Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.CLEANUPAGENT.DELETEWORKFLOWUSER.ActivationMultiplier`	Controls how often workflow components are optimized with respect to users that have been removed from the system.	12
`ECM.AGENT.CLEANUPAGENT.DISABLEDOMAINADMINUSER.ActivationMultiplier`	Controls how often verification is performed for administrative users to ensure that the users still have administration mode access. For users that have lost all administration mode access, the administration representation of the user is disabled, and remains disabled until the user is again granted application administration access, or is removed from the system.	1
`ECM.AGENT.CLEANUPAGENT.EMPTYARCHIVE.ActivationMultiplier`	Controls how often content that has passed the expiration period set by the Content Administrator is deleted from the Archive.	24
`ECM.AGENT.CLEANUPAGENT.EMPTYTRASH.ActivationMultiplier`	Controls how often Trash folders are emptied if they were configured to be automatically emptied.	4
`ECM.AGENT.CLEANUPAGENT.ISSUEDOMAINQUOTAWARNING.ActivationMultiplier`	Controls how often e-mail notification warnings are sent when the quota used by a Site is at or near the allocated quota limit for that Site. E-mail notifications are sent to any users of that Site with the Quota Administrator role, as well as to the administrator e-mail address specified in the `IFS.DOMAIN.EMAIL.AdministratorAddress` domain property.	12
`ECM.AGENT.CLEANUPAGENT.ISSUEDOMAINQUOTAWARNING.ConsumptionPercentageThreshhold`	Specifies how close the used quota for a Site needs to be to the allocation limit for a Site quota warning to be issued. The value is specified as a percentage of the Site quota allocation.	95
`ECM.AGENT.CLEANUPAGENT.ISSUEDOMAINQUOTAWARNING.IncludeArchiveConsumption`	Specifies whether documents in a Site's Archive are considered to count against the quota used for a Site.	true
`ECM.AGENT.CLEANUPAGENT.PURGEDELETEDWORKSPACE.ActivationMultiplier`	Controls how often Libraries that have been deleted and that are unreferenced in the Archive are permanently removed from the system.	24

Content Agent

The Content Agent controls the management of document content when BFILE aging has been set up. When BFILE aging has been enabled, the Content Agent moves content to a BFILE if it has not been accessed after the retention period. See "Managing Storage Options" on page 5-6 for information about setting up BFILE aging.

The default name for this server configuration is:

```
ContentAgentConfiguration
```

Table E–5 lists the properties for the Content Agent.

Table E–5 Content Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENT.CONTENTAGENT.ContentToBfileManager`	The fully qualified classname of the `ContentToBfileManager` interface.	`oracle.ifs.management.servers.content.IfsContentToBfileManager`
`IFS.SERVER.AGENT.CONTENTAGENT.MaxFilesPerFolder`	For every relative path created, the maximum number of files that can be moved to a folder.	500
`IFS.SERVER.AGENT.CONTENTAGENT.MaxFoldersPerActivationPeriod`	The maximum number of folders created when the Content Agent runs.	20
`IFS.SERVER.AGENT.CONTENTAGENT.RetentionPeriod`	How long a file may be kept in the database as a LOB if it is not accessed.	30d

Content Garbage Collection Agent

File attributes and content are stored separately. For performance reasons, the content of a document is not deleted when the document is deleted. The Content Garbage Collection Agent deletes the unreferenced content. Like many agents, this agent runs at a specific time that is specified in the `IFS.SERVER.TIMER.InitialTimeOfDay` and `IFS.SERVER.TIMER.ActivationPeriod` properties.

The default name for this server configuration is:

```
ContentGarbageCollectionAgentConfiguration
```

Table E–6 lists the properties for the Content Garbage Collection Agent.

Table E–6 Content Garbage Collection Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENT.CONTENTGARBAGECOLLECTIONAGENT.FilteredContentRemovalPeriod`	Amount of time filtered content is kept in the system before it is deleted. HTML-generated rendition of content is an example of filtered content. Unit of measure is seconds.	3600
`IFS.SERVER.AGENT.CONTENTGARBAGECOLLECTIONAGENT.FreedContentBatchSize`	The maximum number of unreferenced ContentObjects that are freed in a single iteration of this agent.	10000

Dangling Object AV Cleanup Agent

Similar to the Garbage Collection Agent, the Dangling Object AV Cleanup Agent removes orphaned object type references and identifies all invalid object references, such as references to objects that no longer exist, and sets these references to null for array type attributes and zero for scalar attributes. For example, this agent cleans up the owner attribute of a document pointing to a directory object that was deleted and is no longer valid.

The default name for this server configuration is:

```
DanglingObjectAVCleanupAgentConfiguration
```

Table E–7 lists the properties for the Dangling Object AV Cleanup Agent.

Table E–7 Dangling Object AV Cleanup Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENTS.DANGLINGOBJECTAVCLEANUPAGENT.ExcludedAttributeList`	A list of attributes for which invalid references to LibraryObjects are not cleaned up. Do not delete the default values, so the Garbage Collection Agent can handle deleted users correctly. Add additional attributes as needed.	AUDITENTRY PUBLICOBJECT:OWNER PUBLICOBJECT:DELETOR PUBLICOBJECT:CREATOR PUBLICOBJECT:LASTMODIFIER VERSIONSERIES:RESERVOR

Event Exchanger Agent

The Event Exchanger Agent periodically purges expired events from the event queue.

The default name for this server configuration is:

```
EventExchangerAgentConfiguration
```

Table E–8 lists the properties for the Event Exchanger Agent.

Table E–8 Event Exchanger Agent Configuration Properties

Property	Description and Usage Note	Default
`IFS.SERVER.EventLifespan`	The time, in seconds, after which an event is assumed to have been delivered and become eligible for purging.	1800

Event Handler Agent

The Event Handler Agent provides the ability for customers to write custom code in response to audit events. Classes implementing the `oracle.ifs.fdk.EventHandler` are run using this agent. This agent, unlike most other agents, can be run on more than one middle tier.

See the developer documentation for more information about this agent.

The default name for this server configuration is:

```
EventHandlerAgentConfiguration
```

Expiration Agent

All public objects have an attribute called ExpirationDate. When this date passes, the public objects are automatically deleted. This is handled by the Expiration Agent, which periodically deletes expired objects. If the expiration date of a public object passes, the agent deletes the public object. Like many agents, this agent runs at a specific time that is specified in the `IFS.SERVER.TIMER.InitialTimeOfDay` and `IFS.SERVER.TIMER.ActivationPeriod` properties.

The default name for this server configuration is:

```
ExpirationAgentConfiguration
```

Folder Index Agent

The Folder Index Agent handles additional folder index functions not covered by the Folder Index Analyzer Agent. See the following section for more information about the Folder Index Analyzer Agent.

The default name for this server configuration is:

`FolderIndexAgentConfiguration`

Table E–9 lists the properties for the Folder Index Agent.

Table E–9 Folder Index Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENTS.FOLDERINDEXAGENT.MaxDeferredUpdates`	The maximum number of deferred updates processed in a single iteration of this agent.	5000

Folder Index Analyzer Agent

Oracle Content DB uses an internal mechanism called the folder index to speed up folder-restricted queries. This index is modified every time the folder hierarchy gets changed, to reflect the up-to-date folder hierarchy. However, certain forms of file links may leave the folder index in a less than optimal state. The Folder Index Analyzer Agent runs periodically to detect and correct these states, and returns the folder index to an optimal state.

The default name for this server configuration is:

`FolderIndexAnalyzerAgentConfiguration`

Table E–10 lists the properties for the Folder Index Analyzer Agent. Never modify these values.

Table E–10 Folder Index Analyzer Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENTS.FOLDERINDEXANALYZERAGENT.MaxParentsThreshold`	The threshold for the maximum number of parents after which the folder index is considered less than optimal. This condition is ANDed with the `MaxChildrenThreshold`.	10
`IFS.SERVER.AGENTS.FOLDERINDEXANALYZERAGENT.MaxChildrenThreshold`	The threshold for the maximum number of children after which the folder index is considered less than optimal. This condition is ANDed with the `MaxParentsThreshold`.	10

FTP Server

The Oracle Content DB **FTP** server lets users transfer files between one file system and the Oracle Content DB repository. FTP is particularly useful for bulk transfers.

The FTP server is disabled, by default, after Oracle Content DB is installed and configured. See "Enabling FTP" on page 4-3 for information about enabling the FTP protocol.

The default name for this server configuration is:

`FtpServerConfiguration`

Table E–11 lists the properties for the FTP server.

Table E–11 FTP Server Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.PROTOCOL.FTP.AcceptQueueSize`	The number of server requests backlogged before denying requests. Do not change.	50
`IFS.SERVER.PROTOCOL.FTP.AnonymousAllowed`	If set to true, allows anonymous connections.	false
`IFS.SERVER.PROTOCOL.FTP.BannerText`	The string displayed when the FTP client is started. The FTP Banner only supports ASCII characters, because not all FTP clients can display non-ASCII text.	Oracle Content Database FTP Server ready. Access to this system is limited to authorized users for company business purposes only. Unauthorized access to or use of this system is prohibited and may subject you to civil and criminal prosecution. Use of this system may be monitored for the purpose of maintaining system security, and system information may be accessed or disclosed under limited circumstances.
`IFS.SERVER.PROTOCOL.FTP.CommandCharacterSetIsUserCharacterSet`	If set to true, character set is the same as the **Default Character Set** specified by the user in Globalization Preferences. If set to false, character set is the same as specified in `IFS.SERVER.PROTOCOL.FTP.DefaultCommandCharacterSet`. If no character set is found, character set is the same as specified in the session default for the user specified in `IFS.SERVER.SESSION.User`.	true
`IFS.SERVER.PROTOCOL.FTP.DateFormat`	Specifies the default date format.	MMM dd HH:mm
`IFS.SERVER.PROTOCOL.FTP.DefaultCommandCharacterSet`	Default FTP protocol command character set.	ISO-8859-1
`IFS.SERVER.PROTOCOL.FTP.Localhost`	Optionally, specify the host name if the host has multiple homes in the network.	Default_Hostname
`IFS.SERVER.PROTOCOL.FTP.MaximumConnections`	The maximum number of connections for this FTP server.	100
`IFS.SERVER.PROTOCOL.FTP.Port`	The port on which the server is running.	21 If port 21 is already in use, 2100 is used.
`IFS.SERVER.PROTOCOL.FTP.Timeout`Period	Amount of time between activity before the connection times out; default is 900 seconds or 15 minutes. Unit of measure is milliseconds.	900000

FTPS Server - Explicit

The Oracle Content DB FTPS servers provide support for FTP over SSL. Explicit FTPS secures the connection when the client issues an AUTH command. An Explicit FTPS connection starts out as a regular FTP connection; the connection becomes secure only after the client issues an AUTH command.

The FTPS servers are disabled, by default, after Oracle Content DB is installed and configured. See "Enabling FTPS" on page 4-4 for information about enabling the FTPS protocol.

The Explicit FTPS server contains many of the same properties as the FTP Server. Table E–12 only lists those properties that are specific to Explicit FTPS, and those properties that have different default values. See Table E–11 for information about the other properties.

The default name for this server configuration is:

`FtpsServerExplicitConfiguration`

Table E–12 Explicit FTPS Server Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.PROTOCOL.FTP.Port`	The port on which the server is running.	21
`IFS.SERVER.PROTOCOL.FTPS.SECURITY.IMPLICIT`	Determines whether this FTPS server accepts Implicit FTPS or Explicit FTPS clients.	Set to false by default in the `FtpsServerExplicitConfiguration`.
`IFS.SERVER.PROTOCOL.FTPS.WALLET.Location`	Location of the Wallet file.	`/scripts/cwallet.sso`

FTPS Server - Implicit

The Oracle Content DB FTPS servers provide support for FTP over SSL. Implicit FTPS secures the channel on connection.

The FTPS servers are disabled, by default, after Oracle Content DB is installed and configured. See "Enabling FTPS" on page 4-4 for information about enabling the FTPS protocol.

The Implicit FTPS server contains many of the same properties as the FTP Server. Table E–13 only lists those properties that are specific to Implicit FTPS, along with those properties that have different default values. See Table E–11 for information about the other properties.

The default name for this server configuration is:

`FtpsServerImplicitConfiguration`

Table E–13 Implicit FTPS Server Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.PROTOCOL.FTP.Port`	The port on which the server is running.	990
`IFS.SERVER.PROTOCOL.FTPS.SECURITY.IMPLICIT`	Determines whether this FTPS server accepts Implicit FTPS or Explicit FTPS clients.	Set to true by default in the `FtpsServerImplicitConfiguration`.
`IFS.SERVER.PROTOCOL.FTPS.WALLET.Location`	Location of the wallet file.	`/scripts/cwallet.sso`

Garbage Collection Agent

The Garbage Collection Agent fixes invalid public object owners, creators, and modifiers. For example, a document is created and modified by jsmith. The creator, owner, and last modifier attribute of document are set to the object ID of jsmith. If jsmith is deleted, then the attribute value becomes invalid. The agent replaces these invalid attribute values with the ID of the replacement owner, creator, or modifier specified in the server configuration properties.

The default name for this server configuration is:

`GarbageCollectionAgentConfiguration`

Table E–14 lists the properties for the Garbage Collection Agent.

Table E–14 Garbage Collection Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementOwner`	User to be replaced as owner. Modify as needed.	`system`
`IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementCreator`	User to be replaced as creator. Modify as needed.	`system`
`IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementModifier`	User to be replaced as modifier. Modify as needed.	`system`

HTTP Server

The HTTP server lets users access the Oracle Content DB Web client. It also contains properties for **WebDAV** access.

The default name of this server configuration is:

`EcmHttpServerConfiguration`

Table E–15 lists the properties for the HTTP server.

Table E–15 HTTP Server Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.PROTOCOL.DAV.Browse.Enabled`	If set to true, WebDAV will return a directory listing when a user tries to GET a folder through the WebDAV servlet. If set to false, the user is redirected to the Web interface.	true
`IFS.SERVER.PROTOCOL.DAV.DigestNonceTimeout`	Nonce refers to the challenge used by WebDAV in digest authentication. After using a nonce to authenticate, the client can continue accessing the server until the timeout period is reached, at which point the server sends another challenge and the client must authenticate again. Unit of measure is minutes.	10
`IFS.SERVER.PROTOCOL.DAV.Locks.Timeout.Min`	The minimum timeout value, in seconds, that a client can request when acquiring a lock. This value prevents clients from asking for short timeouts, then refreshing frequently, which increases server load.	601
`IFS.SERVER.PROTOCOL.DAV.Propfind.Infinity.Enabled`	Whether to allow depth-infinity PROPFIND requests on collections, which can be extremely resource-intensive.	true
`IFS.SERVER.PROTOCOL.DAV.Propfind.Infinity.MaxResponses`	The maximum number of results to collect for a depth-infinity PROPFIND on a collection before rejecting the request. This limit only applies to depth-infinity PROPFIND requests; depth-one requests are not affected. Set to -1 to collect unlimited results. This property is ignored if `IFS.SERVER.PROTOCOL.DAV.Propfind.Infinity.Enabled` is set to false.	1001
`IFS.SERVER.PROTOCOL.DAV.Welcome`	The array of welcome document names that are served up if a GET is done on a directory containing one of these documents. Typically used so that `index.html` will be served automatically when the directory is requested. To disable this feature, set to an empty array.	index.html index.htm

Renaming the Oracle Content DB HTTP Server

Do not change the name of the `EcmHttpServer`. If you change the server name, you will not be able to access Oracle Content DB through the Web client.

If you must change the server name, you must also change the name in the `web.xml` configuration file. To change the server name:

1. Rename the server using the Application Server Control.
2. Edit `web.xml`, located in the following directory:

   ```
   ORACLE_HOME/j2ee/OC4J_Content/applications/content/content/WEB-INF/
   ```

   Look for the following lines of code, and replace the value for `<param-value>`:

   ```
   <init-param>
     <param-name>IFS.SERVER.PROTOCOL.DAV.IfsServer.Name</param-name>
     <param-value>EcmHttpServer</param-value>
   </init-param>
   ```

3. Save the file.
4. Restart the OC4J instance.

Inbound Queue Listener Agent

The Inbound Queue Listener Agent is a time-based agent that polls all of the inbound queues periodically so that Oracle Content DB can act upon the messages placed on inbound queues. The Inbound Queue Listener Agent can dequeue a message and delegate the work of processing to the message object itself.

The default name for this server configuration is:

```
InboundQueueListenerAgentConfiguration
```

Table E–16 lists the properties for the Inbound Queue Listener Agent.

Table E–16 Inbound Queue Listener Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENT.INBOUNDQUEUELISTENERAGENT.Queues`	Holds a list of queues on which the agent will listen.	IFS_IN IFS_BPEL_IN

Lock Expiration Agent

The Lock Expiration Agent is a time-based agent that releases locks that are timed out. The agent needs to be running at all times for the automatic expiration function of the lock to work.

The default name for this server configuration is:

```
LockExpirationAgentConfiguration
```

Most Recent Doc Agent

The Most Recent Doc Agent is an event-based agent that reacts to documents that have been uploaded or accessed by each user. The information provided by the agent is used whenever a user accesses My Recent Documents.

The default name for this server configuration is:

```
MostRecentDocAgentConfiguration
```

Table E–17 lists the properties for the Most Recent Doc Agent.

Table E–17 Most Recent Doc Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.MOSTRECENTDOCAGENT.EventBatchSize`	The maximum number of events processed in a single iteration of this agent.	5000

Oracle Event Handler Agent

The Oracle Event Handler Agent is used for all handlers used internally by Oracle. This agent, unlike most other agents, can be run on more than one middle tier.

See the developer documentation for more information about this agent.

The default name for this server configuration is:

```
OracleEventHandlerAgentConfiguration
```

Oracle Internet Directory Credential Manager Agent

The Oracle Internet Directory Credential Manager Agent is a time-based agent that polls for changes to Oracle Internet Directory users. If a user has been added, modified, or deleted in Oracle Internet Directory, the Oracle Internet Directory Credential Manager Agent provisions the change in Oracle Content DB.

Set the `IFS.SERVER.TIMER.ActivationPeriod` property if you want to change how frequently this agent runs. The default is every 15 minutes.

The default name for this server configuration is:

```
OidCredentialManagerAgent
```

Table E–18 lists the properties for the Oracle Internet Directory Credential Manager Agent.

Table E–18 Oracle Internet Directory Credential Manager Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENT.OIDCREDENTIALMANAGERAGENT.MaxEventCount`	Number of events to handle at one time.	100
`IFS.SERVER.AGENT.OIDCREDENTIALMANAGERAGENT.OidChangeHandler`	The fullyqualified classname of the `OidChangeHandler` implementation.	`oracle.ifs.ecm.util.oid.EcmOidChangeHandler`

Quota Agent

The Quota Agent is triggered by an event to compute the quota used for Libraries. This agent also checks all active Libraries periodically, according to a specified timer period. The agent updates the storage used by the Library. When the storage used is over the allocated quota, users of the Library will not be able to add any more documents to that Library. Documents in Trash count toward the quota for a Library.

The quota for a Library is calculated based on the content already used. This means that a Library will go over quota when a user of that Library adds the final file that pushes the storage used over the storage limit. When you set the allocated quota for a

Library, remember that the last file the user puts in the Library must go over quota before being denied.

Quotas will not be enforced if:

- The Quota Agent has not been started or is not running.
- The quota for a Library has not been enabled.

The default name for this server configuration is:

`QuotaAgentConfiguration`

Read Document Agent

The Read Document Agent is an event-based agent that reacts to documents read by users, by triggering a custom workflow if one is configured for the document that is read.

If no custom workflow is configured for the Read Document operation on the folders where the documents are read, the agent takes the action of moving the **BFILE** content of any recently read document back into a **LOB**. Documents are moved to BFILEs by the Content Agent; see "Content Agent" on page E-5 for more information.

The default name for this server configuration is:

`ReadDocumentAgentConfiguration`

Table E–19 lists the properties for the Read Document Agent.

Table E–19 Read Document Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.READDOCUMENTAGENT.EventBatchSize`	The maximum number of events processed in a single iteration of this agent.	5000

Reassign Quota Agent

The Reassign Quota agent is an event-based agent that adjusts the quota charged for content in the system when content is moved between Libraries, often a time-consuming task.

The default name for this server configuration is:

`ReassignQuotaAgentConfiguration`

Table E–20 lists the properties for the Reassign Quota Agent.

Table E–20 Reassign Quota Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.REASSIGNQUOTAAGENT.EventBatchSize`	The maximum number of events processed in a single iteration of this agent.	5000

Records DB HTTP Server

The Records DB HTTP server allows users to access the Oracle Records DB Web client.

The default name for this server configuration is:

`RmHttpServerConfiguration`

Records DB Lifecycle Agent

The Records DB Lifecycle Agent is a time-based agent that processes the cutoff, retention, and disposition instructions on record categories and record folders.

The default name for this server configuration is:

```
RmLifeCycleAgentConfiguration
```

Refresh Security Agent

The Refresh Security Agent is an event-based agent that reacts to changes in grants applied at the Site or Container level, and modifies the security applied lower in the folder hierarchy accordingly, if necessary.

The default name for this server configuration is:

```
RefreshSecurityAgentConfiguration
```

Table E–21 lists the properties for the Refresh Security Agent.

Table E–21 Refresh Security Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.REFRESHSECURITYAGENT.EventBatchSize`	The maximum number of events processed in a single iteration of this agent.	5000

Secure Enterprise Search Group Agent

This agent is not used. Do not activate this agent.

Service Warmup Agent

When a node is started, the Service Warmup Agent automatically preloads the data cache of the service. All properties for this agent are required. Unlike most other agents, this agent is configured to run separately on each node.

The default name for this server configuration is:

```
ServiceWarmupAgentConfiguration
```

Table E–22 lists the properties for the Service Warmup Agent.

Table E–22 Service Warmup Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENT.SERVICEWARMUP.WarmupAcls`	If set to true, preloads ACL collection.	false
`IFS.SERVER.AGENT.SERVICEWARMUP.WarmupFormats`	If set to true, preloads format collection.	true
`IFS.SERVER.AGENT.SERVICEWARMUP.WarmupMedias`	If set to true, preloads Media collection.	true
`IFS.SERVER.AGENT.SERVICEWARMUP.WarmupSetAdmin`	Whether the preloading is done in administration mode.	true
`IFS.SERVER.AGENT.SERVICEWARMUP.WarmupUsers`	If set to true, preloads user collection.	false

Service Watchdog Agent

The Service Watchdog Agent cleans up after Oracle Content DB services that do not shut down cleanly.

The default name for this server configuration is:

`ServiceWatchdogAgentConfiguration`

Table E–23 lists the properties for the Service Watchdog Agent.

Table E–23 Service Watchdog Agent Configuration Properties

Property	Description and Usage Notes	Default
`IFS.SERVER.AGENT.SERVICEWATCHDOGAGENT.ServiceTimeoutPeriod`	The number of seconds after which a service is considered inactive. When a service becomes inactive, it is eligible for cleanup by the Service Watchdog Agent.	120

Statistics Agent

The Statistics agent is a time-based agent that gathers statistics pertaining to service activity on the node where the agent is running. Unlike most other agents, this agent is configured to run separately on each node, so that statistics are gathered independently for each node. The properties of the agent determine whether the statistics are logged, and whether they are written to a document stored in the Oracle Content DB repository.

The default name for this server configuration is:

`StatisticsAgentConfiguration`

Table E–24 lists the properties for the Statistics Agent.

Table E–24 Statistics Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.STATISTICSAGENT.CreateStatisticsDocument`	Specifies whether an HTML document should be created, whose content is the currently gathered statistics. The name for this file is automatically generated and appears as `*node_name_*log.html`.	false
`ECM.AGENT.STATISTICSAGENT.LogStatistics`	If set to true, the currently gathered statistics are sent to the node or application log.	true
`ECM.AGENT.STATISTICSAGENT.StatisticsFolderPath`	The path within the Oracle Content DB folder hierarchy where the statistics document should be created. The path must refer to a Library or a folder within a Library. Do not include a file name as part of this path; the statistics document file name is autogenerated. If the folder where the statistics file resides does not have a versioning policy set on it, the file will be overwritten every time the agent logs statistics. You should set the folder versioning policy to Auto Versioning or Manual Versioning so that a new version is generated each time the agent logs statistics. When you set the versioning policy, be sure to set the **Maximum number of versions to keep** to a high number to ensure that statistics are kept for an adequate time period. For example, if you keep the activation period for this agent at 15 minutes (the default), you would need 96 versions in order to retain statistics for a 24-hour period.	Not applicable

Version Purge Agent

The Version Purge agent is an event-based agent that purges versioned documents that have exceeded the version limit specified by the Versioning Configuration in effect for the documents. The purged versions are moved to the associated Trash folder.

The default name for this server configuration is:

```
VersionPurgeAgentConfiguration
```

Table E–25 lists the properties for the Version Purge Agent.

Table E–25 Version Purge Agent Configuration Properties

Property	Description and Usage Notes	Default
`ECM.AGENT.VERSIONPURGEAGENT.EventBatchSize`	The maximum number of events processed in a single iteration of this agent.	5000

Virus Repair Agent

The Virus Repair Agent is responsible for repairing files that have been infected with a virus, and for retrieving the latest virus definitions. Whenever the agent becomes active, it will poll the SAVSE server for updated virus definitions, and then attempt to repair the quarantined files. The agent will not try to repair the following files:

- Files that have exceeded the maximum number of repair attempts
- Files that have already experienced repair attempts using the current virus definitions

The default name for this server configuration is:

```
VirusRepairAgentConfiguration
```

F

FTP Quote Command Reference

This appendix provides information about using the FTP quote commands.

This appendix provides information about the following topics:

- SETCHARACTERSET
- SETCOMMANDCHARACTERSET
- SETLANGUAGE
- SHOWCHARACTERSET
- SHOWLANGUAGE

SETCHARACTERSET

Sets the character encoding to an IANA character set name for the session when loading documents. Use when loading documents that are different than the default system character encoding setting. The character encoding setting is important for content-based indexing, used for content searches. For more information about character encodings, see *Oracle Database Globalization Support Guide*.

Syntax	**Example**
`quote setcharacterset [character set]`	`quote setcharacterset UTF-8`

Valid character encodings include:

BIG5
BIG5-HKSCS
EUC-JP
EUC-TW
GB2312
GB18030
IBM850
IBM852
IBM857
IBM866
ISO-2022-CN
ISO-2022-JP
ISO-2022-KR
ISO-8859-1
ISO-8859-2
ISO-8859-3
ISO-8859-4
ISO-8859-5
ISO-8859-6
ISO-8859-7
ISO-8859-8
ISO-8859-9
KOI8-R
KS_C_5601-1987
SHIFT_JIS
TIS-620
UTF-8
UTF-16BE
UTF-16LE
WINDOWS-936
WINDOWS-949
WINDOWS-950
WINDOWS-1250
WINDOWS-1251
WINDOWS-1252
WINDOWS-1253
WINDOWS-1254
WINDOWS-1255
WINDOWS-1256
WINDOWS-1257
WINDOWS-1258

SETCOMMANDCHARACTERSET

Sets the command character set for the FTP session. This character set specifies the character encoding to be used in subsequent FTP commands. The FTP protocol server converts FTP commands from this character encoding to Java String and vice versa. When the FTP session is first created, the FTP server uses the default character set of the session. The IANA naming standards should be used to specify the character set. See "SETCHARACTERSET" on page F-1 for a list of valid character encodings.

Syntax	**Example**
`quote setcommandcharacterset [character set]`	`quote setcommandcharacterset UTF-8`

SETLANGUAGE

Sets the language for the session when loading documents. Should be used when loading documents that are different than the default system language. The language setting is important for content-based indexing, used for content searches. For more information on language setting, see *Oracle Database Globalization Support Guide*.

Syntax	**Example**

`quote setlanguage [`*`language`*`]`	`quote setlanguage French`
	`quote setlanguage "Latin American Spanish"`

The list of valid languages is given in the following table. For languages that are longer than one word, the language needs to be enclosed in quotes as shown in the preceding example.

American
Arabic
Bengali
Brazilian Portuguese
Bulgarian
Canadian French
Catalan
Croatian
Czech
Danish
Dutch
Egyptian
English
Estonian
Finnish
French
German
Greek
Hebrew
Hungarian
Indonesian
Italian
Japanese
Korean
Latin American Spanish
Latvian
Lithuanian
Malay
Mexican Spanish
Norwegian
Polish
Portuguese
Romanian
Russian
Simplified Chinese
Slovak
Slovenian
Spanish
Swedish
Thai
Traditional Chinese
Turkish
Ukrainian
Vietnamese

SHOWCHARACTERSET

Displays the both the current command character set and the current document character set of the FTP session.

Syntax	**Example**
`quote showcharacterset`	`quote showcharacterset`

SHOWLANGUAGE

Displays the current language setting for the session.

Syntax	**Example**
`quote showlanguage`	`quote showlanguage`

G

Oracle Content DB Globalization Support

Oracle Content DB globalization support lets users store and search documents of heterogeneous character sets and languages in a single Oracle Content DB instance. The globalization infrastructure ensures that the resource strings, error messages, sort order, date, time, numeric, and calendar conventions adapt automatically to any native language and locale.

Globalization support is provided in the Oracle Content DB repository so that the other dependent processes, such as the protocol servers, can share and use this support. The major globalization goal for the repository is to ensure efficient storage of documents of heterogeneous character sets and languages, and to allow effective update, retrieval, and search operations on these documents.

This appendix provides information about the following topics:

- How to Choose the Database Character Set for Oracle Content DB
- How to Ensure Documents Are Properly Indexed in Oracle Content DB
- Globalization and the Oracle Content DB Protocols
- Character Sets Supported in Oracle Content DB
- Document Languages Supported in Oracle Content DB

How to Choose the Database Character Set for Oracle Content DB

In the repository, all metadata strings, such as the name of the document or the description, are stored in the VARCHAR2 data type of Oracle Database. Strings stored in this data type are encoded in the database character set specified when a database is created. The document itself, however, is unstructured data and stored in one of the large object data types of Oracle Database, particularly the BLOB data type. The BLOB data type stores content as is, avoiding any character set conversion on document content. The LONG and CLOB data types store content in the database character set, which requires character set conversion. Conversions can compromise the data integrity and have the potential to convert incorrectly or lose characters.

The full-text search index built on the document content is encoded in the database character set. When the content of a document is indexed, the BLOB data is converted from the character set of the content to the database character set for creation of the index text tokens. If the character set of the content is not a subset of the database character set, then the conversion will yield garbage tokens. For example, a database character set of ISO-8859-1 (Western European languages) will not be able to index correctly a Shift-JIS (Japanese) document. To be able to search content effectively, the character set of the documents stored by the users must be considered when selecting the database character set.

If your Oracle Content DB instance will contain multilingual documents, AL32UTF-8 is the recommended database character set. AL32UTF-8 supports characters defined in the Unicode standard. The Unicode standard solves the problem of many different languages in the same application or database. Unicode is a single, global character set that contains all major living scripts and conforms to international standards. Unicode provides a unique code value for every character, regardless of the platform, program, or language. AL32UTF-8 is the 8-bit encoding of Unicode. It is a variable-width encoding and a strict superset of ASCII. One Unicode character can be 1 byte, 2 bytes, 3 bytes, or 4 bytes in AL32UTF-8 encoding. Characters from the European scripts are represented in either 1 or 2 bytes. Characters from most Asian scripts are represented in 3 bytes. Supplementary characters are represented in 4 bytes. By using a Unicode-based file system, document content and metadata of different languages can be shared by users with different language preferences in one system.

How to Ensure Documents Are Properly Indexed in Oracle Content DB

To support documents in different character sets and languages in a single file system, the repository associates two globalization attributes with each document. They are the character set and language attributes.

Character Set

The character set of a document is used in several situations. When the document content is rendered to a file, the character set of the document is used as the character encoding of the file. When the document is displayed in the browser, the character set of the document is set in the HTTP content-type header. Finally, when a full-text search is built on a text document, Oracle Text uses the character set of the document to convert the data into the database character set before building the index. When a character set is updated, the content is reindexed.

If no character set is specified when a document is inserted, the repository determines a default character set by using the character set of the user's Library session stored in the Localizer object. This is obtained from the PrimaryUserProfile information of the user when the Library session of the user is initialized.

Language

The language of a document is used as a criterion to limit the search for documents of a particular language. It is also used to build a full-text search index on the document with Oracle Text. The multilexer feature of Oracle Text uses the language to identify the specific lexer to parse the document for searchable words. The language-specific lexers need to be defined and associated with a language before the index is built. Table G–1 describes the language-specific lexers.

Table G–1 Language-Specific Lexers

Language	**Lexer**	**Lexer Option**
Brazilian Portuguese	BASIC_LEXER	BASE LETTER
Canadian French	BASIC_LEXER	BASE LETTER INDEX THEME
Danish	BASIC_LEXER	BASE LETTER DANISH ALTERNATE SPELLING
Dutch	BASIC_LEXER	BASE LETTER
Finnish	BASIC_LEXER	BASE LETTER

Table G–1 (Cont.) Language-Specific Lexers

Language	Lexer	Lexer Option
French	BASIC_LEXER	BASE LETTER INDEX THEME THEME LANGUAGE=FRENCH
German	BASIC_LEXER	BASE LETTER GERMAN ALTERNATE SPELLING
Italian	BASIC_LEXER	BASE LETTER
Japanese	JAPANESE_VGRAM_LEXER	Not applicable
Korean	KOREAN_LEXER	Not applicable
Latin American	BASIC_LEXER	BASE LETTER
Spanish Portuguese	BASIC_LEXER	BASE LETTER
Simplified Chinese	CHINES_VGRAM_LEXER	Not applicable
Swedish	BASIC_LEXER	BASE LETTER SWEDISH ALTERNATE SPELLING
Tradition Chinese	CHINESE_VGRAM_LEXER	Not applicable
Others	BASIC_LEXER	INDEX THEME THEME LANGUAGE=ENGLISH INDEX TEXT

The BASIC_LEXER is used for single-byte languages using white space as a word separator. Asian language lexers cannot use white space as word separators. Instead, they use a V-gram algorithm to parse the documents for searchable keys. Languages that are not supported by Oracle Text are parsed as English. Oracle Content DB uses the multilexer feature of Oracle Text. It is a global lexer that contains German, Danish, Swedish, Japanese, Simplified Chinese, Traditional Chinese, and Korean sublexers.

If no language is specified when a document is inserted, the repository determines a default language as follows:

1. If the character set has been set, the language can most likely be obtained from a best-guess algorithm based on the character set value. For example, a document with a character set of Shift-JIS will most likely be in Japanese.
2. The default language is obtained from the Localizer of the user’s Library session. During initialization of the Library session, the default language is obtained from the PrimaryUserProfile of the user.
3. The default language and default character set are specified when a new user is created in Oracle Internet Directory.

Oracle Content DB identifies languages using Oracle Globalization Support language abbreviations. See "Document Languages Supported in Oracle Content DB" on page G-7 for a list of Oracle Content DB-supported languages.

Globalization and the Oracle Content DB Protocols

Some protocols do not support multibyte user names. Access through WebDAV and HTTP is not available for user names that contain multibyte characters. FTP allows multibyte user names. In addition, some protocols require that user passwords be in ASCII format.

For FTP, you can use a protocol command character set that is different from the default document character set. A *protocol command character set* is the character set you use to enter commands in FTP or other protocols.

FTP

Oracle Content DB provides the following server configuration properties to specify the default FTP command character set:

- `IFS.SERVER.PROTOCOL.FTP.DefaultCommandCharacterSet`
- `IFS.SERVER.PROTOCOL.FTP.CommandCharacterSetIsUserCharacterSet`

The following precedence model determines a session's FTP command character encoding:

1. Explicitly specified (using `quote setcommandcharacterset`).
2. If `IFS.SERVER.PROTOCOL.FTP.CommandCharacterSetIsUserCharacterSet` is true, then use the default character set specified in the user's Oracle Internet Directory profile.
3. If `IFS.SERVER.PROTOCOL.FTP.CommandCharacterSetIsUserCharacterSet` is false, then use the value of `IFS.SERVER.PROTOCOL.FTP.DefaultCommandCharacterSet`.
4. If no character set is found, then use the value of the session default for the user specified in `IFS.SERVER.SESSION.User`.

The standard FTP protocol does not define the character set of the file names or directory names that are usually passed as arguments of FTP commands. The FTP server is responsible for interpreting the byte sequence of the FTP commands. To allow users to access documents of different character sets and languages, and to allow users to set and view the protocol command character set, the Oracle Content DB FTP server provides the following QUOTE commands:

- **`Ftp> quote setcommandcharacterset`:** Lets users specify the command character set for the FTP session. This character set specifies the character encoding to be used in subsequent FTP commands. The FTP protocol server converts FTP commands from this character encoding to Java String and the reverse. When the FTP session is first created, the FTP server uses the default character set of the session. Use the IANA naming standards to specify the character set.
- **`Ftp> quote setcharacterset`:** Lets users specify the character set of the documents to be uploaded. Called `setcharencoding` in previous releases of Oracle Content DB. Use the IANA naming standards to specify the character set.
- **`Ftp> quote showcharacterset`:** Displays both the current command character set and the current document character set of the FTP session. Called `showcharencoding` in previous releases of Oracle Content DB. The character set is displayed in the IANA naming standards.
- **`Ftp> quote setlanguage`:** Lets users specify the language for the FTP session. The language of an FTP session is then associated with the documents that are uploaded. Oracle Text uses the language information to determine the appropriate lexer to use to index the document. When the FTP session is first created, the FTP server uses the default language of the session. Use Oracle language names.
- **`Ftp> quote showlanguage`:** Displays the current language of the FTP session. The language is displayed with the Oracle naming standard.

When a quote command is issued to change the character set or language of the FTP session, the FTP server updates the settings in the Localizer object of the current Library session. Subsequently, because quote commands cannot be issued until an FTP session is established, only user names in the character set or subset of the FTP server's default character set can be used to log in to the FTP server. See Appendix F, "FTP Quote Command Reference" for more information about quote commands.

Users can specify the character sets and languages of their environments using standard command-line FTP clients. Browser-based FTP clients, such as Internet Explorer or Netscape, do not allow quote commands to be used. FtpSession defaults will be used.

Character Sets Supported in Oracle Content DB

Table G–2 is a summary of the character sets supported in Oracle Content DB.

Table G–2 Character Sets Supported in Oracle Content DB

Language	IANA Preferred MIME Character Set	IANA Additional Aliases	Java Encodings	Oracle Character Set
Arabic (ISO)	iso-8859-6	ISO_8859-6:1987, iso-ir-127, ISO_8859-6, ECMA-114, ASMO-708, arabic, csISOLatinArabic	ISO8859_6	AR8ISO8859P6
Arabic (Windows)	windows-1256	none	Cp1256	AR8MSWIN1256
Baltic (ISO)	iso-8859-4	csISOLatin4, iso-ir-110, ISO_8859-4, ISO_8859-4:1988, l4, latin4	ISO8859_4	NEE8ISO8859P4
Baltic (Windows)	windows-1257	none	Cp1257	BLT8MSWIN1257
Central European (DOS)	ibm852	cp852, 852, csPcp852	Cp852	EE8PC852
Central European (ISO)	iso-8859-2	csISOLatin2, iso-ir-101, iso8859-2, iso_8859-2, iso_8859-2:1987, l2, latin2	ISO8859_2	EE8ISO8859P2
Central European (Windows)	windows-1250	x-cp1250	Cp1250	EE8MSWIN1250
Chinese	iso-2022-cn It is not defined in IANA, but use in MIME documents.	csISO2022CN	ISO2022CN	ISO2022-CN
Chinese Simplified (GB2312)	gb2312	chinese, csGB2312, csISO58GB231280, GB2312, GB_2312-80, iso-ir-58	EUC_CN	ZHS16CGB231280
Chinese Simplified (GB18030)	GB18030	none	GB18030	ZHS32GB18030
Chinese Simplified (Windows)	GBK	windows-936	GBK	ZHS16GBK
Chinese Traditional	big5	csbig5, x-x-big5	Big5	ZHT16BIG5

Table G–2 (Cont.) Character Sets Supported in Oracle Content DB

Language	IANA Preferred MIME Character Set	IANA Additional Aliases	Java Encodings	Oracle Character Set
Chinese Traditional	windows-950	none	MS950	ZHT16MSWIN950
Chinese Traditional (EUC-TW)	EUC-TW	none	EUC_TW	ZHT32EUC
Chinese Traditional (Big5-HKSCS)	Big5-HKSCS	none	Big5_HKSCS	ZHT16HKSCS
Cyrillic (DOS)	ibm866	cp866, 866, csIBM866	Cp866	RU8PC866
Cyrillic (ISO)	iso-8859-5	csISOLatinCyrillic, cyrillic, iso-ir-144, ISO_8859-5, ISO_8859-5:1988	ISO8859_5	CL8ISO8859P5
Cyrillic (KOI8-R)	koi8-r	csKOI8R, koi	KOI8_R	CL8KOI8R
Cyrillic Alphabet (Windows)	windows-1251	x-cp1251	Cp1251	CL8MSWIN1251
Greek (ISO)	iso-8859-7	csISOLatinGreek, ECMA-118, ELOT_928, greek, greek8, iso-ir-126, ISO_8859-7, ISO_8859-7:1987, csISOLatinGreek	ISO8859_7	EL8ISO8859P7
Greek (Windows)	windows-1253	none	Cp1253	EL8MSWIN1253
Hebrew (ISO)	iso-8859-8	csISOLatinHebrew, hebrew, iso-ir-138, ISO_8859-8, visual, ISO-8859-8 Visual, ISO_8859-8:1988	ISO8859_8	IW8ISO8859P8
Hebrew (Windows)	windows-1255	none	Cp1255	IW8MSWIN1255
Japanese (JIS)	iso-2022-jp	csISO2022JP	ISO2022JP	ISO2022-JP
Japanese (EUC)	euc-jp	csEUCPkdFmtJapanese, Extended_UNIX_Code_Packed_Format_for_Japanese, x-euc, x-euc-jp	EUC_JP	JA16EUC
Japanese (Shift-JIS)	shift_jis	csShiftJIS, csWindows31J, ms_Kanji, shift-jis, x-ms-cp932, x-sjis	MS932	JA16SJIS
Korean	ks_c_5601-1987	csKSC56011987, korean, ks_c_5601, euc-kr, csEUCKR	EUC_KR	KO16KSC5601
Korean (ISO)	iso-2022-kr	csISO2022KR	ISO2022KR	ISO2022-KR
Korean (Windows)	windows-949	none	MS949	KO16MSWIN949
South European (ISO)	iso-8859-3	ISO_8859-3, ISO_8859-3:1988, iso-ir-109, latin3, l3, csISOLatin3	ISO8859_3	SE8ISO8859P3
Thai	TIS-620	windows-874	TIS620	TH8TISASCII
Turkish (Windows)	windows-1254	none	Cp1254	TR8MSWIN1254
Turkish (ISO)	iso-8859-9	latin5, l5, csISOLatin5, ISO_8859-9, iso-ir-148, ISO_8859-9:1989	ISO8859_9	WE8ISO8859P9

Table G–2 (Cont.) Character Sets Supported in Oracle Content DB

Language	IANA Preferred MIME Character Set	IANA Additional Aliases	Java Encodings	Oracle Character Set
Universal (UTF-8)	utf-8	unicode-1-1-utf-8, unicode-2-0-utf-8, x-unicode-2-0-utf-8	UTF8	UTF8
Unicode (UTF-16BE)	UTF-16BE	none	UTF-16BE	AL16UTF16
Unicode (UTF-16LE)	UTF16LE	none	UTF-16LE	AL16UTF16LE
Vietnamese (Windows)	windows-1258	none	Cp1258	VN8MSWIN1258
Western Alphabet	iso-8859-1	cp819, ibm819, iso-ir-100, iso8859-1, iso_8859-1, iso_8859-1:1987, latin1, l1, csISOLatin1	ISO8859_1	WE8ISO8859P1
Western Alphabet (DOS)	ibm850	cp850, 850, csIBM850	Cp850	WE38PC850
Western Alphabet (Windows)	windows-1252	x-ansi	Cp1252	WE8MSWIN1252

Document Languages Supported in Oracle Content DB

Table G–3 is a summary of the document languages supported in Oracle Content DB. Note that the supported document languages are different from the languages supported in the Oracle Content DB application.

Table G–3 Document Languages Supported in Oracle Content DB

Oracle Language Name	Java Locale	ISO Locale
Arabic	ar	ar
Bengali	bn	bn
Brazilian Portuguese	pt_BR	pt-br
Bulgarian	bg	bg
Canadian French	fr_CA	fr-CA
Catalan	ca	ca
Croatian	hr	hr
Czech	cs	cs
Danish	da	da
Dutch	nl	nl
Egyptian	ar_EG	ar-eg
American	en	en
English	en_GB	en-gb
Estonian	et	et
Finnish	fi	fi
French	fr	fr
German	de	de

Table G–3 (Cont.) Document Languages Supported in Oracle Content DB

Oracle Language Name	Java Locale	ISO Locale
Greek	el	el
Hebrew	he	he
Hungarian	hu	hu
Icelandic	is	is
Indonesian	id	in
Italian	it	it
Japanese	ja	ja
Korean	ko	ko
Latin American Spanish	es	es
Latvian	lv	lv
Lithuanian	lt	lv
Malay	ms	ms
Mexican Spanish	es_MX	es-mx
Norwegian	no	no
Polish	pl	pl
Portuguese	pt	pt
Romanian	ro	ro
Russian	ru	ru
Simplified Chinese	zh_CN	zh-cn
Slovak	sk	sk
Slovenian	sl	sl
Spanish	es_ES	es-es
Swedish	sv	sv
Thai	th	th
Traditional Chinese	zh_TW	zh-tw
Turkish	tr	tr
Ukrainian	uk	uk
Vietnamese	vi	vi

Glossary

administrator

One of two types of administrators in Oracle Content DB: **system administrators** or **application administrators**.

Administration Mode

Provides access to Oracle Content DB application administration functions such as allocating quota and assigning roles.

Advanced Queuing (AQ)

Provides an infrastructure for distributed applications to communicate asynchronously using messages. Advanced Queuing is built into Oracle Database and supports sophisticated queuing features, including subscriptions, inter-queue message propagation, message latency, message expiration, structured payloads, and exception queues. Full name: Oracle Streams Advanced Queueing.

agents

Processes that perform operations periodically (time-based) or in response to events generated by other Oracle Content DB servers or processes (event-based). An agent is a type of Oracle Content DB **server**.

application administrators

Administrators who are responsible for tasks related to a particular **Site**, such as managing users, quotas, categories, and content. There are a variety of application administration roles, including User Administrator, Category Administrator, Container Administrator, Content Administrator, and Quota Administrator. See *Oracle Content Database Application Administrator's Guide* for more information about application administration roles and tasks.

Application Server Control

A Web-based management interface used to manage Oracle Application Server middle-tier hosts. Oracle Content DB system administrators can use the Application Server Control to operate and monitor system processes associated with the Oracle Content DB **domain** and **nodes**. Full name: Oracle Enterprise Manager 10*g* Application Server Control.

Archive

Location where items are stored that have been deleted from user or Library trash. Each **Site** contains an Archive folder. Depending on how the Site has been configured, items in the Archive may be automatically deleted after a specified period of time.

Files and folders in the Archive can be restored by the Content Administrator of the Site.

BFILE

A read-only Oracle data type consisting of a directory object and a file name. Oracle Content DB provides transparent access to content stored as either a **BLOB** (online storage) or a BFILE (near-line storage). If BFILEs are enabled for your Oracle Content DB **domain**, you can configure content archiving or content aging.

BLOB

A type of large object (**LOB**) provided by the database. All documents in Oracle Content DB are stored as BLOBs. Full name: binary large object.

BPEL

An XML-based markup language for composing a set of discrete Web services into an end-to-end process flow. Full name: Business Process Execution Language. See also **Oracle BPEL Process Manager**.

Committed Data Cache

A feature that provides caching of the attribute values of frequently used objects without a database request, greatly improving performance and scalability.

custom workflow

A customized workflow process created in the BPEL Designer (a component of **Oracle BPEL Process Manager**). Custom workflows must be registered with Oracle Content DB before they can be used.

domain

A logical grouping of Oracle Content DB **nodes**, and an Oracle Database instance that contains the Oracle Content DB data.

domain properties

Settings that apply to the entire Oracle Content DB **domain**. For example, the domain property `IFS.DOMAIN.SEARCH.AttemptContextSearchRewrite` determines whether or not Oracle Content DB tries to generate fast-response SQL for text searches.

EMC Centera

A partner solution that provides retention hardware support. You can integrate Oracle Content DB with EMC Centera to provide retention storage for **Oracle Records DB**.

formats

Attributes that indicate document file type (for example, .doc or .zip). The format of a document determines how its content is indexed. Also known as MIME types.

FTP

One of three **protocols** supported by Oracle Content DB, used for file transfers across wide area networks, such as the Internet. **FTPS** is also supported. Full name: File Transfer Protocol.

FTPS

FTP over SSL. FTPS defines a mechanism to implement the FTP Security Extensions based on the TLS protocol. Two types of FTPS are supported by Oracle Content DB:

- Implicit FTPS secures the channel on connection.

- Explicit FTPS (Auth TLS) secures the connection when the client issues an AUTH command. An Explicit FTPS connection starts out as a regular FTP connection; the connection becomes secure only after the client issues an AUTH command.

Do not confuse FTPS with SFTP, a service of the Secure Shell that is not related to FTP.

Grid Control

The Grid Control is a Web-based management interface used for centralized management of Oracle Application Server middle tiers, OracleAS Infrastructure tiers, and Oracle Database hosts. Oracle Content DB system administrators can use the Grid Control for access to Oracle Content DB metrics, such as document statistics, node statistics, and users, including access to historical metric data. Full name: Oracle Enterprise Manager 10*g* Grid Control.

HTTP

One of three **protocols** supported by Oracle Content DB, used for Web-based access. HTTP has been extended with **WebDAV**, a protocol designed for wide area networks such as the Internet. Full name: Hypertext Transfer Protocol.

HTTP nodes

One of two types of Oracle Content DB **nodes**. The Oracle Content DB HTTP node runs as part of an **OC4J** process called `OC4J_Content`. The **Oracle Records DB** HTTP node runs as part of an OC4J process called `OC4J_RM`. Through servlets that are configured to work with OC4J, the HTTP nodes provide the following support:

- The Oracle Content DB HTTP node supports the Oracle Content DB application, **WebDAV**, and Web services.
- The Oracle Records DB HTTP node supports the Oracle Records DB application WebDAV, and Web services.

identity management

The process by which various components in an identity management system manage the security life cycle for network entities in an organization. Most commonly refers to the management of application users in an enterprise organization. See also **Oracle Identity Management**.

Libraries

Configurable folders for storing and sharing content with an allocated quota.

LDAP

An Internet protocol that applications use to look up contact information from a server, such as a central directory. LDAP servers index all the data in their entries, and filters can be used to select just the person or group you want, and return just the information you want. Full name: Lightweight Directory Access Protocol.

LOB

The majority of data stored in Oracle Content DB is stored as LOBs in database tablespaces. Full name: large object.

loggers

Functional areas with configurable logging levels for each **node**. For example, you can specify a more detailed level of logging for a particular protocol server or agent logger in which you are interested.

Network Appliance SnapLock

A partner solution that provides retention hardware support. You can integrate Oracle Content DB with Network Appliance SnapLock to provide retention storage for Oracle Records DB.

nodes

The application software that comprises the product, along with the underlying Java Virtual Machine (JVM) required to support the software at runtime. There are two types of nodes: **regular nodes**, and **HTTP nodes**. Each node is based on a particular **node configuration**.

node configuration

A configuration object that specifies the run-time behavior of a particular **node**. Each node has its own corresponding node configuration. If you want to make permanent changes to a node, such as changing **servers** or **services**, modify the node configuration for the node. If you want to make temporary (run-time) changes to a node, modify the node itself. Changes made at run time are lost when the node is restarted. You cannot create a node directly; instead, you must first create an active node configuration, and then a corresponding node will be created automatically.

node manager

The actual process that gets started when a **node** is started. It is responsible for starting the default **service** and **servers** for a node. It also provides an administrative API for the node that lets you to find information about node log levels, locale information, available free memory, and the Oracle home of the node.

OC4J

A complete set of J2EE containers written entirely in Java that run on the Java Virtual Machine (JVM) of the standard Java Development Kit (JDK). OC4J supplies the following J2EE containers: a servlet container that complies with the servlet 2.3 specification, and a JSP container that complies with the Sun JSP 1.2 specification. Full name: Oracle Application Server Containers for J2EE.

OPMN

Manages all the components within an application server instance, including **Oracle HTTP Server**, **OC4J** processes, and OracleAS **Web Cache**. It channels all events from different components to all components interested in receiving them. Use OPMN to manage Oracle Content DB processes like **HTTP nodes** and **regular nodes**. Full name: Oracle Process Manager and Notification Server.

OracleAS Infrastructure

An application server installation type that provides centralized product metadata and security services, configuration information, and data repositories for Oracle Application Server middle tiers. Oracle Content DB middle tiers use the OracleAS Infrastructure for three main services: Product Metadata Service, **Oracle Identity Management** Services, and the Management Service. Full name: Oracle Application Server Infrastructure.

Oracle BPEL Process Manager

A component of Oracle Application Server. It includes the BPEL Server, the BPEL Console, the BPEL Worklist application for human-centric workflows, and the BPEL Designer. You can use the BPEL Designer, an Oracle JDeveloper-based design tool, to graphically create custom workflows for use in Oracle Content DB. See also **BPEL**.

Oracle Content Management SDK

A robust development platform for content management applications that was used to build Oracle Content DB. Oracle CM SDK provides a set of Java APIs that expose file system functionality such as file storage and searching, as well as document delete, move, and rename operations. The APIs also provide content management features unique to Oracle CM SDK, such as document versioning, controlling access to documents, and advanced queuing to facilitate communication between applications.

Oracle Drive

Oracle Drive is a native Windows application that lets users use Windows Explorer, Microsoft Office, and other Windows applications to access content in Oracle Content DB. Oracle Drive displays files and folders in Oracle Content DB as a mapped drive in Windows Explorer. Oracle Drive also provides an effective offline solution that lets users edit files on their computers when offline, and then synchronize with the server when they reconnect.

Oracle Enterprise Manager

A systems management software application that enables you to manage and monitor Oracle Application Server instances and other Oracle server products. See also **Application Server Control**.

Oracle HTTP Server

The Web server component of Oracle Application Server, based on the Apache HTTP Server, version 1.3.28. Do not confuse with the Oracle Content DB HTTP protocol server (`EcmHttpServer`).

Oracle Identity Management

An integrated set of components that provide distributed security to Oracle products and make it possible to centrally and securely manage enterprise identities and their access to applications in the enterprise. It includes the following components: **Oracle Internet Directory**, Oracle Directory Integration and Provisioning, Oracle Delegated Administration Services, OracleAS **Single Sign-On**, and Oracle Application Server Certificate Authority.

Oracle Internet Directory

An **LDAP** service that combines Oracle Database technology with the LDAP v3 directory standard. Oracle Internet Directory is a component of **Oracle Identity Management**. It is also closely integrated with Oracle Database. All Oracle Content DB users are created and managed in Oracle Internet Directory.

Oracle RAC

Two or more computers configured to interact to provide the appearance of a single Oracle Database. These two or more nodes are linked by an interconnect. The interconnect serves as the communication path between each node in the cluster database. Each Oracle instance uses the interconnect for the messaging that synchronizes each instance's use of shared resources. Oracle also uses the interconnect to transmit data blocks that are shared by the multiple instances. The datafiles accessed by all the nodes are the primary type of shared resource. Oracle RAC requires that all nodes have simultaneous access to the shared disks to give the instances concurrent access to the database. Full name: Oracle Real Application Cluster.

Oracle Records DB

A component of Oracle Content DB that provides support for compliance solutions such as enforced record creation and retention policies. Records Administrators can use Oracle Records DB to specify file plans and create record categories.

Oracle Text

A full-text retrieval technology built into Oracle Database for indexing and searching text and documents. Oracle Text supports mixed languages and character sets in the same index. Oracle Content DB uses the text indexing and retrieval features of Oracle Text. To enable content-based searching, Oracle Text indexes each file you store in Oracle Content DB.

Oracle Workflow

A system that supports business process definition, automation, and integration. Its technology enables automation and continuous improvement to business processes, by routing information of any type according to user-defined rules. The internal Oracle Content DB workflows, such as Request for Quota, were created in Oracle Workflow. The two default approvals workflow processes, Parallel Vote and Serial Approval, were also created in Oracle Workflow.

OUI

The installation wizard through which you can install Oracle products, including Oracle Database and Oracle Application Server. Full name: Oracle Universal Installer.

protocols

Means by which users can connect to Oracle Content DB. Oracle Content DB supports three protocols: **FTP**, **HTTP**, and **WebDAV**. The Oracle Content DB protocol servers listen for requests from clients on a specific port and respond to requests according to the rules of the protocol specification. Each protocol may interact with Oracle Content DB in a different way. A protocol server is a type of Oracle Content DB **server**.

quote commands

Special FTP commands that you can use with the Oracle Content DB **FTP** server. They include `SETCHARACTERSET`, `SETCOMMANDCHARACTERSET`, `SETLANGUAGE`, `SHOWCHARACTERSET`, and `SHOWLANGUAGE`.

Read-Only Connection Pool

A set of database connections shared by the **sessions** to perform database read operations. A minimum number of connections are created when the **service** is started. Depending on the number of concurrent operations performed by the sessions, and the nature of these operations, additional connections may be added to the pool, up to a specified maximum. See also **Writable Connection Pool**.

realms

A collection of identities and associated policies that is typically used when enterprises want to isolate user populations and enforce different identity management policies for each population. Oracle Content DB **Sites** are based on realms. Realms are created and managed in **Oracle Internet Directory**. Also known as identity management realms.

regular nodes

One of two types of Oracle Content DB **nodes**. The regular node supports protocol servers, such as **FTP**, and **agents**, such as the Garbage Collection Agent. You can configure additional regular nodes on the same computer or on additional computers.

SAVSE

A partner solution that provides options to verify that content is virusfree and to clean files that are found to be infected. After antivirus integration has been enabled and configured, files are scanned for viruses whenever they are opened for read access, using the latest available virus definitions. Full name: Symantec AntiVirus Scan Engine.

schema

A collection of database objects, including logical structures such as tables, views, sequences, stored procedures, synonyms, indexes, clusters, and database links. A schema has the name of the database user who controls it. The Oracle Content DB schema is created in an Oracle database during the configuration process. The schema owns all database objects, including metadata about Oracle Content DB and configuration information.

servers

Processes that support protocol access to Oracle Content DB (protocol servers) or that perform important internal functions (**agents**). Each Oracle Content DB **node** can support multiple servers. Each server is based on a particular **server configuration**.

server configuration

A configuration object that holds the default values used when a **server** is started for an Oracle Content DB **node**. In addition to the server type, each server configuration specifies values for parameters relevant to that type. For example, the **FTP** server configuration specifies the FTP port number, whether anonymous FTP connections are allowed, and the connection timeout period. If you want to make permanent changes to a server, modify its server configuration. If you want to make temporary (run-time) changes to a server, modify the server itself. Changes made to servers at run time are lost when the node is restarted.

services

Processes that manage user **sessions** and that allow those sessions to access data in the Oracle Content DB repository. Each **node** must have at least one active service. A node can support multiple services, but typically you require only one for each node. Each service is based on a particular **service configuration**.

service configuration

A configuration object that holds the default values used when a **service** is started for an Oracle Content DB **node**. There are three default service configurations, named to reflect the size of their data caches: SmallServiceConfiguration, MediumServiceConfiguration, and LargeServiceConfiguration. If you want to make permanent changes to a service, modify its service configuration. If you want to make temporary (run-time) changes to a service, modify the service itself. Changes made to services at runtime are lost when the node is restarted.

sessions

There are two types of sessions in Oracle Content DB: user sessions, and Library sessions.

User sessions are specific connections of a user to Oracle Content DB through a user process. A user session is not always initiated by a user; for example, a user session could be started by an agent acting on behalf of a user, or a user being logged in through a persistent cookie. A user session lasts from the time the user logs in until the time the user logs out, or until the session times out. User sessions are subject to limits based on the Maximum Sessions Per User set for each node.

Library sessions manage user transactions and are supported by Oracle Content DB **services**. Library sessions are subject to limits based on the Maximum Concurrent Requests Per User set for each node, as well as the service configuration property `IFS.SERVICE.MaximumConcurrentSessions`, which limits Library sessions across all users for a particular service.

Single Sign-On

A component of Oracle Application Server that enables users to log in to multiple applications using a single user name and password. Oracle Content DB users log in to Oracle Content DB using their **SSO password**. Full name: Oracle Application Server Single Sign-On.

SSO password

The password assigned to each Oracle Content DB user in **Oracle Internet Directory**. Users provide this password to authenticate against the OracleAS **Single Sign-On** server. Oracle Content DB users use the SSO password to sign in to Oracle Content DB. Full name: Single Sign-On password.

Sites

A discrete organizational entity in Oracle Content DB whose users can collaborate on files and folders. Users in one Site do not have access to the content of users in another Site. Oracle Content DB Sites are based on **realms**.

system administrators

Administrators in Oracle Content DB that are typically responsible for the following tasks:

- Installing and configuring Oracle Content DB
- Customizing their Oracle Content DB deployment by enabling Oracle Records DB, virus checking, the FTP server, BFILE storage, retention hardware, or other options
- Managing the Oracle Content DB domain, nodes, services, and servers
- Performing system tuning and troubleshooting
- Adding, deleting, and managing Sites
- Registering custom workflows

tablespace

A database storage unit that groups related logical structures together.

Web Folders

The Microsoft operating system extension that supports the **WebDAV** protocol. Using Web Folders, you can drag and drop files into Oracle Content DB and browse your files through Windows Explorer. On Microsoft Windows 2000 and Microsoft Windows XP, Web Folders appears in Network Places.

WebDAV

One of three **protocols** supported by Oracle Content DB. It lets clients browse and edit files on Oracle Content DB as if they were on the local machine. WebDAV is designed for wide area networks such as the Internet. Currently, the most widespread WebDAV client is the **Web Folders** extension to Windows Explorer, also known as Network Places in Windows 2000/XP. **Oracle Drive** uses WebDAV as its back-end protocol.

Oracle Content DB also provides WebDAV support for Macintosh users. Full name: Web-based Distributed Authoring and Versioning.

Web Cache

A component of Oracle Application Server that improves the performance, scalability, and availability of frequently used Web sites. By storing frequently accessed URLs in memory, OracleAS Web Cache eliminates the need to repeatedly process requests for those URLs on the Web server. OracleAS Web Cache uses invalidation-based caching. Full name: Oracle Application Server Web Cache.

workflow designer

A person with the necessary skills to design a workflow process in Oracle BPEL Process Manager. The workflow designer creates the **custom workflow** process, then the system administrator registers the custom workflow process with Oracle Content DB.

Writable Connection Pool

A set of database connections shared by the **sessions** to perform database read and write operations within a database transaction. A minimum number of connections are created when the **service** is started. Depending on the number of concurrent operations performed by the sessions, and the nature of these operations, additional connections may be added to the pool up to a specified maximum. See also **Read-Only Connection Pool**.

Index