

## **Oracle® Files**

Administrator's Guide

Release 2 (9.0.4)

**Part No. B10872-02**

April 2004

Oracle Files Administrator's Guide, Release 2 (9.0.4)

Part No. B10872-02

Copyright © 2002, 2004, Oracle. All rights reserved.

Primary Author: Marla Azriel

Contributing Authors: Neal Kaplan, Alan Wiersba

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

---

---

# Contents

<b>Send Us Your Comments .....</b>	<b>xiii</b>
<b>Preface .....</b>	<b>xv</b>
Audience .....	xv
Organization .....	xvi
Related Documentation .....	xviii
Conventions .....	xix
Documentation Accessibility .....	xxii
 <b>1 Oracle Files Concepts</b>	
<b>Oracle Files Architecture.....</b>	<b>1-1</b>
Built With Oracle Content Management SDK .....	1-1
The Oracle Files Domain .....	1-2
Oracle Files Schema .....	1-2
Oracle Files Nodes .....	1-2
Services, Servers, and Agents.....	1-5
Oracle Internet Directory .....	1-5
The Subscriber Model.....	1-6
<b>Oracle Files Features .....</b>	<b>1-6</b>
Three Levels of Administration .....	1-7
Workspaces .....	1-7
Workspace Access Levels .....	1-7
Workspace Quota.....	1-7
File Management.....	1-8
Searching .....	1-8
Categories .....	1-8
Versioning .....	1-8
Review Process .....	1-8
Custom Review Processes .....	1-9
Trash.....	1-9
Edit-in-Place.....	1-9
File Synchronization .....	1-9
<b>Integration with Key Oracle Technologies.....</b>	<b>1-9</b>
Integration With Oracle Collaboration Suite .....	1-10
Integration with Oracle9i Database Server.....	1-10

Oracle9i Database and the Oracle Files Schema .....	1-10
Oracle Text .....	1-10
Oracle Advanced Queueing .....	1-10
Oracle9i Real Application Clusters (RAC) .....	1-10
Integration with Oracle9i Application Server .....	1-11
Oracle9iAS Containers for J2EE (OC4J) .....	1-11
Oracle Enterprise Manager .....	1-11
Oracle Internet Directory .....	1-13
Oracle Workflow .....	1-13

## 2 Oracle Files Protocol Support

<b>Industry-Standard Protocol Servers</b> .....	2-1
<b>Client Software and Access Paths</b> .....	2-2
Oracle FileSync Client Software .....	2-2
Installing Oracle FileSync .....	2-2
Client Access Paths .....	2-2
AppleTalk Filing Protocol (AFP) Access for Macintosh Clients .....	2-3
HTTP (Web Browser) and WebDAV Access .....	2-3
SMB/NTFS Access .....	2-4
FTP Access .....	2-4
NFS (Network File System) Protocol Access .....	2-4
<b>Using Oracle Files with NFS</b> .....	2-8
Configuring the NFS Server .....	2-8
Mapping UNIX UIDs to Oracle Files User Accounts .....	2-9
Setting Up a Trusted Client List .....	2-10
Enabling NIS Authentication .....	2-11

## 3 Oracle Files Administrative Roles and Tasks

<b>Administrative Roles Quick Reference</b> .....	3-1
Administrative Accounts .....	3-2
<b>System Administrator</b> .....	3-3
Skills Required to Administer Oracle Files .....	3-3
<b>Site Administrator</b> .....	3-4
Managing Subscribers .....	3-5
Creating, Modifying, and Deleting Subscribers .....	3-5
Enabling and Disabling Subscribers .....	3-5
Specifying Notification and Archive Settings .....	3-5
E-mailing a Subscriber .....	3-5
Viewing Subscriber Statistics .....	3-5
Resetting a Subscriber Administrator Password .....	3-5
Registering Custom Workflows .....	3-5
<b>Subscriber Administrator</b> .....	3-6
Setting Defaults .....	3-6
Specifying Default User Settings .....	3-6
Specifying Notification Settings .....	3-6
Specifying Default Quota Settings .....	3-7
Specifying Default Public Folder Settings .....	3-7

Specifying Default Language Settings .....	3-7
Subscriber Information Tasks.....	3-7
Viewing Subscriber Statistics .....	3-7
Requesting to Modify Subscriber's Settings .....	3-7
Contacting the Site Administrator.....	3-7
User Management Tasks .....	3-7
Creating and Provisioning Users.....	3-7
E-mailing Users .....	3-8
Modifying User Information .....	3-8
Updating User Quota .....	3-9
Enabling and Disabling Users .....	3-9
Deleting Users .....	3-9
Category Management Tasks.....	3-9
Creating Categories .....	3-9
Modifying Categories.....	3-9
Deleting Categories.....	3-9
Trash Management Tasks .....	3-9
Archival File and Folder Management Tasks .....	3-9
Recovering a File at a User's Request.....	3-10
Restoring a File or Folder from the Archive .....	3-10
Workspace and File Management Tasks .....	3-10
Working with Workspaces .....	3-10
Updating Workspace Quota.....	3-10
Locking and Unlocking Files.....	3-10

## 4 Administration Tools Overview

<b>Oracle Files Configuration Assistant .....</b>	<b>4-1</b>
Running the Oracle Files Configuration Assistant.....	4-2
<b>Management Tools .....</b>	<b>4-2</b>
Oracle Enterprise Manager Web Site .....	4-2
Using the Oracle Enterprise Manager Web Site to Manage Oracle Files.....	4-3
Oracle Enterprise Manager 10g Grid Control .....	4-4
Accessing the Grid Control .....	4-4
Administration Tabs in Oracle Files.....	4-5
Oracle Directory Manager .....	4-5
<b>Scripts .....</b>	<b>4-5</b>
<b>Bulk Administration Tools for Oracle Files .....</b>	<b>4-6</b>
Running the Bulk Administration Tools .....	4-6
User Administration Tool .....	4-7
Sample XML File .....	4-7
DTD for the User Administration Tool.....	4-7
Troubleshooting the User Administration Tool .....	4-8
Workspace Administration Tool.....	4-8
Sample XML File .....	4-8
DTD for the Workspace Administration Tool .....	4-9
Troubleshooting the Workspace Administration Tool.....	4-10

## 5 Managing the Oracle Files Domain

<b>About the Oracle Files Domain .....</b>	<b>5-1</b>
<b>Starting and Stopping the Oracle Files Domain .....</b>	<b>5-2</b>
<b>Migrating the Domain Controller.....</b>	<b>5-3</b>
Migrating the Domain Controller to a New Middle-Tier Host.....	5-4
Migrating the Domain Controller to an Existing Middle-Tier Host.....	5-4
<b>Managing the Node Processes .....</b>	<b>5-5</b>
Managing Regular Nodes .....	5-5
Starting Regular Nodes .....	5-5
Stopping Regular Nodes .....	5-5
Managing HTTP Nodes .....	5-5
Starting HTTP Nodes .....	5-5
Stopping HTTP Nodes .....	5-5
Permanently Deleting an HTTP Node.....	5-6
<b>Starting, Stopping, Suspending, and Resuming Servers .....</b>	<b>5-6</b>
Loading and Unloading Servers .....	5-7
<b>Managing the Oracle Files Domain from the Command Line .....</b>	<b>5-8</b>
Managing OC4J Processes .....	5-9
<b>Oracle Process Management and Notification .....</b>	<b>5-9</b>

## 6 Changing Configuration Settings

<b>About Configuration Settings .....</b>	<b>6-1</b>
<b>Domain Properties .....</b>	<b>6-1</b>
Changing Domain Properties.....	6-1
<b>Node Configuration.....</b>	<b>6-3</b>
Changing a Node Configuration .....	6-3
Creating a Regular Node Configuration .....	6-5
Creating an HTTP Node Configuration .....	6-6
Deleting a Node Configuration.....	6-7
<b>Service Configuration.....</b>	<b>6-8</b>
Changing a Service Configuration .....	6-8
Creating a Service Configuration.....	6-9
Runtime Service Configuration.....	6-10
About the Committed Data Cache .....	6-10
About the Read-Only Connection Pool .....	6-10
About the Writable Connection Pool .....	6-10
Dynamically Changing Data Cache and Connection Pool Configuration .....	6-11
<b>Server Configuration .....</b>	<b>6-13</b>
Abstract vs. Non-abstract Server Configuration .....	6-14
Change Values of Properties .....	6-15
View Inherited Properties.....	6-15
Changing a Server Configuration.....	6-15
Creating a Server Configuration.....	6-15
Reloading Servers.....	6-16
Deleting a Server .....	6-17
Deleting a Server Configuration .....	6-17
<b>Oracle Files Configuration Options .....</b>	<b>6-17</b>

Oracle Collaboration Suite Search Configuration .....	6-17
Configuring Search Parameters .....	6-18
Printing Services.....	6-19
Notes .....	6-19
MIME Type Formats.....	6-20
<b>Running Oracle Files on Port 80.....</b>	<b>6-22</b>
Changing the Port Number in Oracle Workflow .....	6-22
Changing the Port Number in Oracle9iAS Web Cache.....	6-23
Changing the Port Number in Oracle HTTP Server .....	6-23
Registering the New Port with Oracle9iAS Single Sign-On .....	6-23
Running the Single Sign-On Registration Tool .....	6-23
Restarting the Oracle HTTP Server .....	6-24
Updating the Base Server Configuration and Restarting OC4J .....	6-25
 <b>7   Monitoring Domain, Node, and Service Performance</b>	
<b>Monitoring Domain Performance.....</b>	<b>7-1</b>
<b>Monitoring Node Performance.....</b>	<b>7-3</b>
<b>Monitoring Service Performance .....</b>	<b>7-3</b>
<b>Viewing Log Files.....</b>	<b>7-4</b>
Oracle Enterprise Manager Web Site Logs and Grid Control Logs.....	7-4
Oracle Files Logs .....	7-4
<b>Accessing Metrics and Monitoring Metric Alerts.....</b>	<b>7-5</b>
The Grid Control Management Agent .....	7-5
Managing Oracle Files with the Grid Control .....	7-6
Accessing the Grid Control.....	7-6
Changing the Default Metric Collection Behavior .....	7-6
Reconfiguring Oracle Files (oracle_ifs) Targets in the Grid Control.....	7-6
Viewing Oracle Files Metrics in the Grid Control.....	7-7
Using the Groups Subtab.....	7-7
Using the Search Function.....	7-7
Metric Thresholds and Metric Collection Intervals .....	7-8
Metric Collection Intervals .....	7-8
 <b>8   Oracle Files Security</b>	
<b>Authentication Using Oracle Internet Directory .....</b>	<b>8-1</b>
<b>Protocol Servers .....</b>	<b>8-1</b>
FTP and AFP .....	8-1
HTTP/DAV.....	8-2
Network Channel Encryption .....	8-2
Oracle Files-Specific Passwords .....	8-2
<b>Other Security Issues.....</b>	<b>8-2</b>
Administration Interfaces .....	8-2
JDBC .....	8-3
Oracle Internet Directory .....	8-3
Client Software .....	8-3
<b>Setting Up Oracle Files to Use SSL.....</b>	<b>8-3</b>

Configuring the Oracle Files Application to use SSL .....	8-3
Providing SSL Information During Oracle Files Configuration .....	8-3
Providing SSL Information Post-Configuration.....	8-4
Connecting to Oracle Internet Directory Using SSL .....	8-5
Providing Oracle Internet Directory SSL Information During Oracle Files Configuration.....	8-5
Providing Oracle Internet Directory SSL Information Post-Configuration .....	8-5
<b>Changing the Oracle Files Site Administrator Password .....</b>	<b>8-6</b>
<b>Changing the Oracle Files System Password.....</b>	<b>8-7</b>
Encrypting the System Password in targets.xml .....	8-7
<b>Changing the Oracle Files Schema Password.....</b>	<b>8-8</b>

## 9 Maintenance and Tuning

<b>Backup and Recovery .....</b>	<b>9-1</b>
<b>LOB (Large Objects) Management.....</b>	<b>9-1</b>
Moving Content Off-line or Near-line .....	9-2
Moving Content to BFILES .....	9-2
Disabling the BFILE Agents .....	9-2
<b>Performance Tuning.....</b>	<b>9-3</b>
Run the Oracle Files analyze.sql Script Frequently.....	9-3
Restoring Prior Statistics .....	9-4
Provide Adequate Storage to Improve Performance .....	9-4
Document Storage and Sizing Issues .....	9-4
Oracle Files Metadata and Infrastructure.....	9-6
<b>Analyzing Performance Problems .....</b>	<b>9-6</b>
If the Database is the Bottleneck .....	9-6
If the Java Processes are the Bottleneck .....	9-7
Obtaining Oracle Files Java Cache Statistics.....	9-7

## 10 Customizing Oracle Files

<b>Branding the Oracle Files User Interface.....</b>	<b>10-1</b>
Colors .....	10-1
Fonts .....	10-2
Images .....	10-2
Title Bar.....	10-3
Limitations on Oracle Files Customizations .....	10-3
<b>Using Custom Workflows in Oracle Files .....</b>	<b>10-4</b>
About Custom Workflows.....	10-4
Creating the Workflow Process Definition.....	10-4
The Launch Event .....	10-5
The Workflow Process URL .....	10-5
The Process Status Event .....	10-6
The Response Event.....	10-6
The Cancel Event.....	10-6
Creating the Launch, Response, and Cancel Events.....	10-6
Creating Event Subscriptions for the Launch, Response, and Cancel Events.....	10-6
Registering a Custom Workflow with Oracle Files.....	10-7



Registering a Workflow Process Definition .....	10-7
Editing a Registered Workflow Process Definition .....	10-7
Deleting a Registered Workflow Process Definition .....	10-8
Setting Up E-Mail Notifications in Oracle Workflow .....	10-8
Setting Up UNIX Sendmail.....	10-8
Setting Up the Oracle Workflow Notification Mailer.....	10-9
Creating a Configuration File for the Oracle Workflow Notification Mailer.....	10-10
Starting the Oracle Workflow Notification Mailer .....	10-11
<b>11 Troubleshooting</b>	
Troubleshooting General Problems.....	11-1
<b>A Oracle Text Reference</b>	
Oracle Text Tablespaces and Disk Utilization .....	A-1
Creating and Maintaining the Oracle Text Index.....	A-2
Maintaining the IFS_TEXT Index By Using the Oracle Text PL/SQL Packages .....	A-2
Sync Job .....	A-3
Optimize Job .....	A-3
Monitoring DBMS_JOBS.....	A-3
Changing or Removing the Default DBMS_JOBS.....	A-3
Manually Synchronizing and Optimizing IFS_TEXT.....	A-4
Monitoring Oracle Text Indexing of Oracle Files Documents.....	A-4
Indexing Non-Standard Content Types.....	A-4
Modifying the Search Timeout Parameter .....	A-5
Troubleshooting Oracle Text Problems.....	A-5
<b>B Service Configuration Reference</b>	
<b>C Server Configuration Properties</b>	
Access Control List Index Agent .....	C-2
AppleTalk Filing Protocol (AFP) Server .....	C-2
Content Garbage Collection Agent.....	C-3
Dangling Object AV Cleanup Agent.....	C-3
Distributed Authoring and Versioning (DAV) Server Configuration .....	C-4
Event Exchanger Agent .....	C-4
Expiration Agent.....	C-5
File Transfer Protocol (FTP) Server .....	C-5
Files Base Server Configuration .....	C-6
Files-Specific Server Configuration .....	C-7
Folder Index Analyzer Agent.....	C-8
Garbage Collection Agent .....	C-9
Inbound Queue Listener Agent.....	C-9
Lock Agent.....	C-9
NbServer [NetBIOS] .....	C-9
Network File System (NFS) Protocol Server .....	C-10
NT File System (NTFS) Protocol Server .....	C-12

Print Agent.....	C-13
Quota Agent .....	C-13
Service Warmup Agent.....	C-13
Service Watchdog Agent .....	C-14
Server Message Block (SMB) Protocol Server .....	C-14

## **D Setting Up Oracle Files With RAC**

About Oracle9i Real Application Clusters.....	D-1
Oracle Files Load Balancing and Failover in a RAC Environment .....	D-2
Client Load Balancing .....	D-2
Connect Time Failover .....	D-3
Transparent Application Failover .....	D-4
Listener Load Balancing.....	D-4
Recommended Load Balancing Configuration .....	D-5
Oracle Files Connect Descriptor Settings for RAC.....	D-5
Oracle Files Configuration Tasks for RAC.....	D-6
Preconfiguration Tasks.....	D-6
Setting MAX_COMMIT_PROPAGATION_DELAY .....	D-6
Setting JOB_QUEUE_PROCESSES.....	D-6
Creating a TNS Entry in tnsnames.ora .....	D-6
Configuration Tasks.....	D-7
Post-Configuration Tasks.....	D-7
Adding a <DatabaseUrl> Entry to registry.xml .....	D-7
RAC Settings for Grid Control.....	D-7

## **E Migrating Data to Oracle Files**

Migrating Data from Other File Servers.....	E-1
Server Consolidation Checklist.....	E-1
Migrating Users.....	E-1
Creating Workspaces.....	E-1
Scripted Workspace Creation.....	E-1
Migrating Content.....	E-2
Protocols for Copying Data .....	E-2

## **F FTP Quote Command Reference**

CASCADEOFF .....	F-1
CASCADEON .....	F-1
DELIM .....	F-1
SETLANGUAGE .....	F-2
SETCHARENCODING.....	F-2
SHOWCHARENCODING .....	F-3
SHOWLANGUAGE.....	F-3

## **G Globalization Support**

Globalization Support Overview.....	G-1
The Repository .....	G-1

How to Choose the Database Character Set for Oracle Files .....	G-1
How to Make Sure Documents Are Properly Indexed in Oracle Files .....	G-2
Character Set .....	G-2
Language .....	G-3
Service Configuration Properties.....	G-4
<b>Oracle Files Protocols .....</b>	<b>G-4</b>
FTP.....	G-4
SMB .....	G-5
<b>Character Sets Supported in Oracle Files .....</b>	<b>G-5</b>
<b>Languages Supported In Oracle Files .....</b>	<b>G-7</b>

## **Index**



---

---

# Send Us Your Comments

## **Oracle Files Administrator's Guide, Release 2 (9.0.4)**

**Part No. B10872-02**

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, please indicate the title and part number of the documentation and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: [ifsdoc\\_us@oracle.com](mailto:ifsdoc_us@oracle.com)
- FAX: 650-506-7104 Attn: Oracle Files Documentation Manager
- Postal service:

Oracle Corporation  
Oracle Internet File System  
500 Oracle Parkway, Mailstop 50p4  
Redwood Shores, CA, 94065  
USA

If you would like a reply, please give your name, address, telephone number, and electronic mail address (optional).

If you have problems with the software, please contact your local Oracle Support Services.



---

# Preface

Part of the Oracle Collaboration Suite, Oracle Files is a hosted content management application that supports user collaboration and file sharing. Oracle Files provides a sophisticated, Web-based user interface that enables users to easily share files of any kind with others in a workspace or across an enterprise.

Oracle Files runs with Oracle9i Application Server and an Oracle9i database, and provides a highly scalable content management repository. This guide describes administration functions for Oracle Files.

This preface contains these topics:

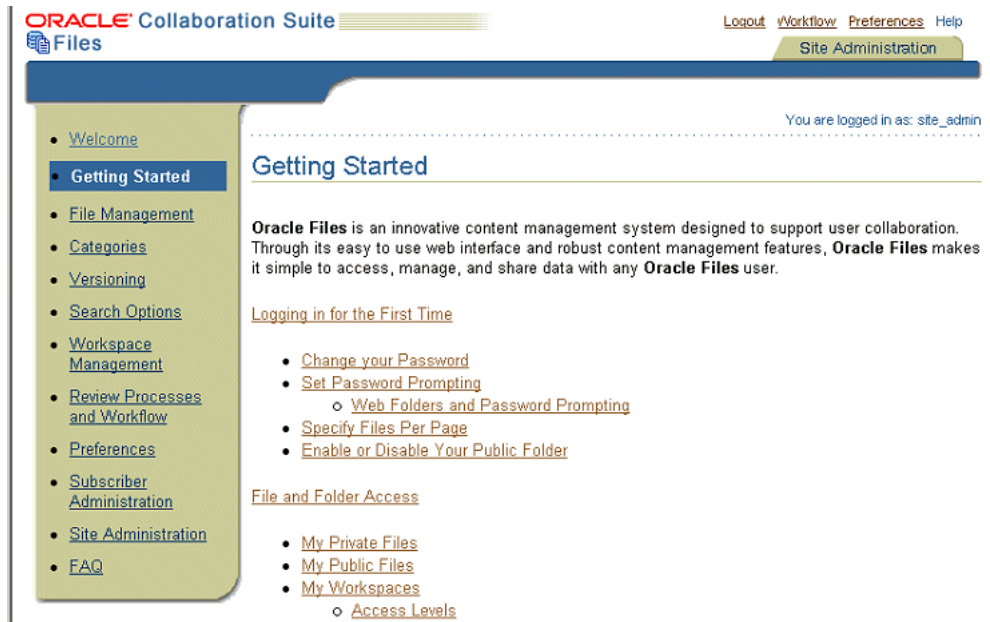
- [Audience](#)
- [Organization](#)
- [Related Documentation](#)
- [Conventions](#)
- [Documentation Accessibility](#)

## Audience

The *Oracle Files Administrator's Guide* is intended for System Administrators, Site Administrators, Subscriber Administrators, or anyone involved in configuring, running, and maintaining an Oracle Files instance.

Additional information for administrators can be found in the Oracle Files online help. To access online help:

1. On any Oracle Files page, click the Help icon. A table of contents appears.
2. You can only view topics for administrators if you are logged in as an administrator. Subscriber Administrators can view the Subscriber Administration topic link; Site Administrators can view both the Subscriber Administration and Site Administration topic links.



Online help is also available in Oracle Enterprise Manager. To access Oracle Enterprise Manager online help:

1. On any Oracle Enterprise Manager page, click **Help**. A table of contents appears.
2. Click **Managing Oracle Files**. The Oracle Files-specific help appears.



## Organization

This document contains:

### Chapter 1, "Oracle Files Concepts"

Introduces the components of Oracle Files, functions, and administration concepts and terminology. Also summarizes the key Oracle technologies with which Oracle Files is integrated.



## **Chapter 2, "Oracle Files Protocol Support"**

Discusses the protocols supported by Oracle Files and shows how to specify access paths for the client software.

## **Chapter 3, "Oracle Files Administrative Roles and Tasks"**

Describes the administrative roles and the basic tasks associated with each role.

## **Chapter 4, "Administration Tools Overview"**

Provides an overview of the tools provided to administer Oracle Files, including the bulk administration tools.

## **Chapter 5, "Managing the Oracle Files Domain"**

Covers runtime processes such as starting and stopping the domain controller, regular nodes, and HTTP nodes.

## **Chapter 6, "Changing Configuration Settings"**

Explains how to change Domain, Node, Service, and Server Configuration parameters.

## **Chapter 7, "Monitoring Domain, Node, and Service Performance"**

Shows how to monitor domain, node, and service performance.

## **Chapter 8, "Oracle Files Security"**

Covers important security topics such as authentication, changing administrative passwords, and protocol limitations.

## **Chapter 9, "Maintenance and Tuning"**

Discusses several methods for optimizing performance and scalability.

## **Chapter 10, "Customizing Oracle Files"**

Discusses branding the Oracle Files user interface and creating custom workflows.

## **Chapter 11, "Troubleshooting"**

Provides information for solving administrative and globalization problems.

## **Appendix A, "Oracle Text Reference"**

Explains strategies for maintaining the Oracle Text index.

## **Appendix B, "Service Configuration Reference"**

Describes the service configuration properties.

## **Appendix C, "Server Configuration Properties"**

Describes the server configuration properties.

## **Appendix D, "Setting Up Oracle Files With RAC"**

Explains how to set up Oracle Files for use with RAC.

## **Appendix E, "Migrating Data to Oracle Files"**

Provides advice on how to migrate from other file systems to Oracle Files.

## **Appendix F, "FTP Quote Command Reference"**

Provides a description, syntax, and example of each FTP Quote command.

## **Appendix G, "Globalization Support"**

Contains information on globalization issues.

## **Related Documentation**

For more information, see these Oracle resources:

### **Oracle Collaboration Suite**

- *Oracle Collaboration Suite Installation and Configuration Guide*
- *Oracle Collaboration Suite Quick Installation Guide*
- *Oracle Collaboration Suite Release Notes*
- *Oracle Files Planning Guide*
- *Oracle Collaboration Suite Using Oracle Files*

### **Oracle9i Application Server**

- *Oracle9i Application Server Concepts*
- *Oracle9i Application Server Installation Guide*
- *Oracle9i Application Server Administrator's Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle HTTP Server Administrator's Guide*
- *Oracle9iAS Single Sign-On Administrator's Guide*
- *Oracle Enterprise Manager Concepts*

### **Oracle9i Database Server**

- *Oracle9i Database Administrator's Guide*
- *Oracle9i Backup and Recovery Concepts*
- *Oracle9i Net Services Administrator's Guide*
- *Oracle9i Globalization Support Guide*
- *Oracle Workflow Guide*

Printed documentation is available for sale in the Oracle Store at

<http://oraclestore.oracle.com/>

To download free release notes, installation documentation, white papers, or other collateral, please visit the Oracle Technology Network (OTN). You must register online before using OTN; registration is free and can be done at

<http://otn.oracle.com/membership/>

If you already have a user name and password for OTN, then you can go directly to the documentation section of the OTN Web site at

<http://otn.oracle.com/docs/index.htm>

To access the database documentation search engine directly, please visit

## Conventions

This section describes the conventions used in the text and code examples of this documentation set. It describes:

- [Conventions in Text](#)
- [Conventions in Code Examples](#)
- [Conventions for Windows Operating Systems](#)

### Conventions in Text

We use various conventions in text to help you more quickly identify special terms. The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
<b>Bold</b>	Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.	When you specify this clause, you create an <b>index-organized table</b> .
<i>Italics</i>	Italic typeface indicates book titles or emphasis.	<i>Oracle9i Database Concepts</i> Ensure that the recovery catalog and target database do <i>not</i> reside on the same disk.
UPPERCASE monospace (fixed-width) font	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, RMAN keywords, SQL keywords, SQL*Plus or utility commands, packages and methods, as well as system-supplied column names, database objects and structures, user names, and roles.	You can specify this clause only for a NUMBER column.  You can back up the database by using the BACKUP command.  Query the TABLE_NAME column in the USER_TABLES data dictionary view.  Use the DBMS_STATS.GENERATE_STATS procedure.
lowercase monospace (fixed-width) font	Lowercase monospace typeface indicates executables, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as user-supplied database objects and structures, column names, packages and classes, user names and roles, program units, and parameter values.  <b>Note:</b> Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	Enter sqlplus to open SQL*Plus.  The password is specified in the orapwd file.  Back up the datafiles and control files in the /disk1/oracle/dbs directory.  The department_id, department_name, and location_id columns are in the hr.departments table.  Set the QUERY_REWRITE_ENABLED initialization parameter to true.  Connect as oe user.  The JReplUtil class implements these methods.
<i>lowercase italic monospace (fixed-width) font</i>	Lowercase italic monospace font represents placeholders or variables.	You can specify the <i>parallel_clause</i> .  Run <i>Uold_release</i> .SQL where <i>old_release</i> refers to the release you installed prior to upgrading.

## Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL\*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
[ ]	Brackets enclose one or more optional items. Do not enter the brackets.	DECIMAL( <i>digits</i> [ , <i>precision</i> ])
{ }	Braces enclose two or more items, one of which is required. Do not enter the braces.	{ENABLE   DISABLE}
	A vertical bar represents a choice of two or more options within brackets or braces. Enter one of the options. Do not enter the vertical bar.	{ENABLE   DISABLE} [COMPRESS   NOCOMPRESS]
...	Horizontal ellipsis points indicate either: <ul style="list-style-type: none"><li>■ That we have omitted parts of the code that are not directly related to the example</li><li>■ That you can repeat a portion of the code</li></ul>	CREATE TABLE ... AS subquery; SELECT col1, col2, ... , coln FROM employees;
. . . . . .	Vertical ellipsis points indicate that we have omitted several lines of code not directly related to the example.	SQL> SELECT NAME FROM V\$DATAFILE; NAME ----- --  /fs1/dbs/tbs_01.dbf /fs1/dbs/tbs_02.dbf  . . .  /fs1/dbs/tbs_09.dbf 9 rows selected.
Other notation	You must enter symbols other than brackets, braces, vertical bars, and ellipsis points as shown.	acctbal NUMBER(11,2); acct CONSTANT NUMBER(4) := 3;
<i>Italics</i>	Italicized text indicates placeholders or variables for which you must supply particular values.	CONNECT SYSTEM/ <i>system_password</i> DB_NAME = <i>database_name</i>

Convention	Meaning	Example
UPPERCASE	Uppercase typeface indicates elements supplied by the system. We show these terms in uppercase in order to distinguish them from terms you define. Unless terms appear in brackets, enter them in the order and with the spelling shown. However, because these terms are not case sensitive, you can enter them in lowercase.	<pre>SELECT last_name, employee_id FROM employees;</pre> <pre>SELECT * FROM USER_TABLES;</pre> <pre>DROP TABLE hr.employees;</pre>
lowercase	<p>Lowercase typeface indicates programmatic elements that you supply. For example, lowercase indicates names of tables, columns, or files.</p> <p><b>Note:</b> Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.</p>	<pre>SELECT last_name, employee_id FROM employees;</pre> <pre>sqlplus hr/hr</pre> <pre>CREATE USER mjjones IDENTIFIED BY ty3MU9;</pre>

## Conventions for Windows Operating Systems

The following table describes conventions for Windows operating systems and provides examples of their use.

Convention	Meaning	Example
Choose <b>Start &gt; menu item</b>	How to start a program.	To start the Database Configuration Assistant, choose <b>Start &gt; Programs &gt; Oracle - HOME_NAME &gt; Configuration and Migration Tools &gt; Database Configuration Assistant</b> .
File and directory names	File and directory names are not case sensitive. The following special characters are not allowed: left angle bracket (<), right angle bracket (>), colon (:), double quotation marks ("), slash (/), pipe ( ), and dash (-). The special character backslash (\) is treated as an element separator, even when it appears in quotes. If the file name begins with \\, then Windows assumes it uses the Universal Naming Convention.	c:\winnt\"system32 is the same as C:\WINNT\SYSTEM32
C:\>	Represents the Windows command prompt of the current hard disk drive. The escape character in a command prompt is the caret (^). Your prompt reflects the subdirectory in which you are working. Referred to as the <i>command prompt</i> in this manual.	C:\oracle\oradata>

Convention	Meaning	Example
Special characters	The backslash (\) special character is sometimes required as an escape character for the double quotation mark (") special character at the Windows command prompt. Parentheses and the single quotation mark (') do not require an escape character. Refer to your Windows operating system documentation for more information on escape and special characters.	C:\>exp scott/tiger TABLES=emp  QUERY=\"WHERE job='SALESMAN' and sal<1600\"  C:\>imp SYSTEM/password FROMUSER=scott  TABLES=(emp, dept)
<i>HOME_NAME</i>	Represents the Oracle home name. The home name can be up to 16 alphanumeric characters. The only special character allowed in the home name is the underscore.	C:\> net start OracleHOME_ NAMETNSListener
<i>ORACLE_HOME</i> and <i>ORACLE_BASE</i>	<p>In releases prior to Oracle8i release 8.1.3, when you installed Oracle components, all subdirectories were located under a top level <i>ORACLE_HOME</i> directory that by default used one of the following names:</p> <ul style="list-style-type: none"> <li>■ C:\orant for Windows NT</li> <li>■ C:\orawin98 for Windows 98</li> </ul> <p>This release complies with Optimal Flexible Architecture (OFA) guidelines. All subdirectories are not under a top level <i>ORACLE_HOME</i> directory. There is a top level directory called <i>ORACLE_BASE</i> that by default is C:\oracle. If you install the latest Oracle release on a computer with no other Oracle software installed, then the default setting for the first Oracle home directory is C:\oracle\orann, where <i>nn</i> is the latest release number. The Oracle home directory is located directly under <i>ORACLE_BASE</i>.</p> <p>All directory path examples in this guide follow OFA conventions.</p> <p>Refer to <i>Oracle9i Database Getting Started for Windows</i> for additional information about OFA compliances and for information about installing Oracle products in non-OFA compliant directories.</p>	Go to the <i>ORACLE_BASE\ORACLE_HOME\rdms\admin</i> directory.

## 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. 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 additional information, visit the Oracle Accessibility Program Web site at

<http://www.oracle.com/accessibility/>

**Accessibility of Code Examples in Documentation** JAWS, a Windows screen reader, 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, JAWS may not always read a line of text that consists solely of a bracket or brace.





---

# Oracle Files Concepts

Oracle Files is designed as an enterprise file server replacement, with added content management features (for example, versioning) that enable users to collaborate more productively. All content is stored in an Oracle database.

No additional client software is required, unless you choose to run Oracle FileSync, the file synchronization tool. Oracle FileSync must be installed separately on each client in order to be used.

Oracle Files provides:

- Support for file-sharing and collaboration protocols.
- A Web user interface designed for large-scale deployments.
- Workspace-based collaboration.
- Content management features like extensible metadata, versioning, and content-based searching.
- Workflow integration for approval and routing.
- User and administrator options for single file recovery.
- Scalability, reliability, security, and platform independence.

These features and capabilities are designed to help IT managers lower costs through file server consolidation while simultaneously making employees more productive.

This chapter discusses basic concepts you should understand when administering Oracle Files. Topics include:

- [Oracle Files Architecture](#)
- [Oracle Files Features](#)
- [Integration with Key Oracle Technologies](#)

## Oracle Files Architecture

The following sections describe the technology underlying Oracle Files, as well as how the domain controller, nodes, and other processes interact. It also provides information about Oracle Internet Directory and the Oracle Files Subscriber model.

## Built With Oracle Content Management SDK

Oracle Files was built using the Oracle Content Management Software Development Kit (Oracle CM SDK), a robust development platform for content management applications.

It 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

You can find more information about Oracle Content Management SDK at:

<http://otn.oracle.com/products/ifs>

## The Oracle Files Domain

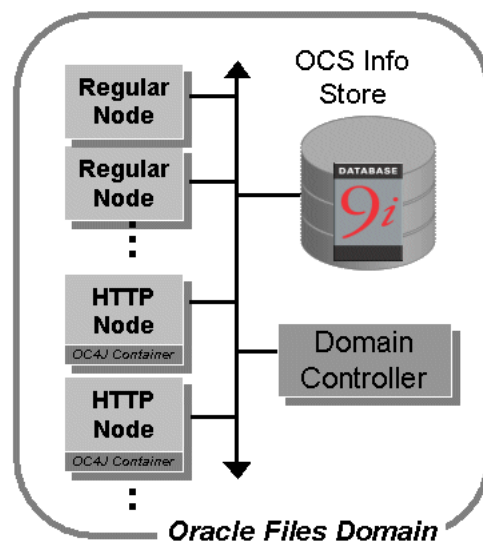
An Oracle Files *domain* is a logical grouping of Oracle Files nodes, running under the control of the domain controller process, and an Oracle9i database instance (called the "Oracle Collaboration Suite Information Store") that contains the Oracle Files data. The nodes and domain controller process run on Oracle9i Application Server.

### Oracle Files Schema

The Oracle Files schema is created in an Oracle database during the configuration process. The schema owns all database objects, including metadata about Oracle Files and configuration information (see [Figure 1-1](#)).

An Oracle Files *node* is the application software that comprises the product, along with the underlying Java Virtual Machine (JVM) required to support the software at runtime. The Oracle Files domain controller process controls and manages the nodes making up the domain.

**Figure 1-1 The Oracle Files Domain**



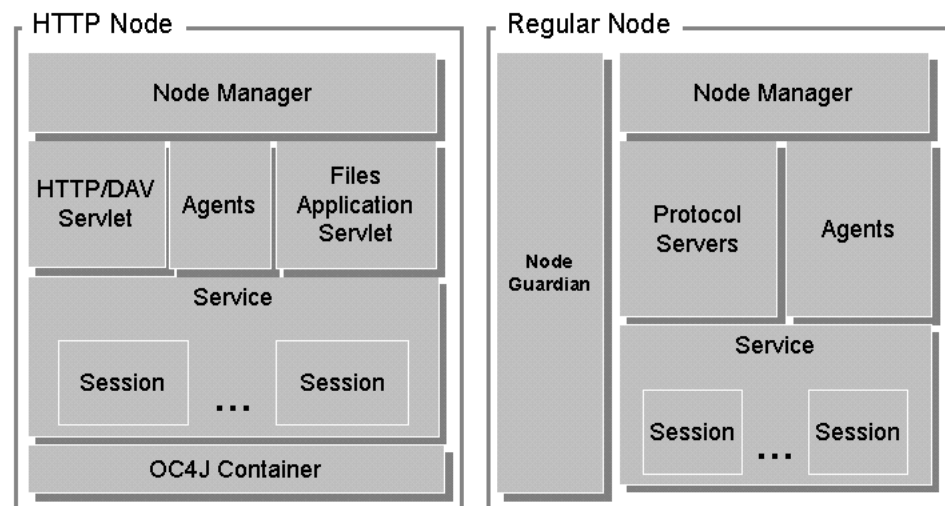
### Oracle Files Nodes

Important concepts to understand about nodes include:

- An Oracle Files domain encompassing any number of nodes is controlled by one (and only one) domain controller process.
- An Oracle Files domain includes two nodes by default: one regular node and one HTTP node (see [Figure 1-2](#)). You can configure additional regular nodes on the same computer or on additional computers.

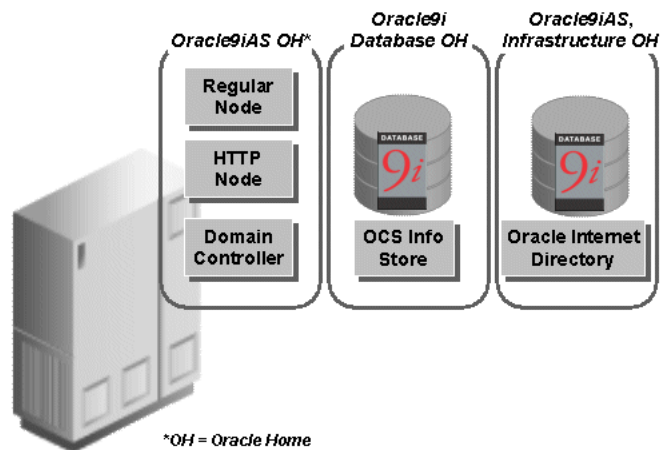
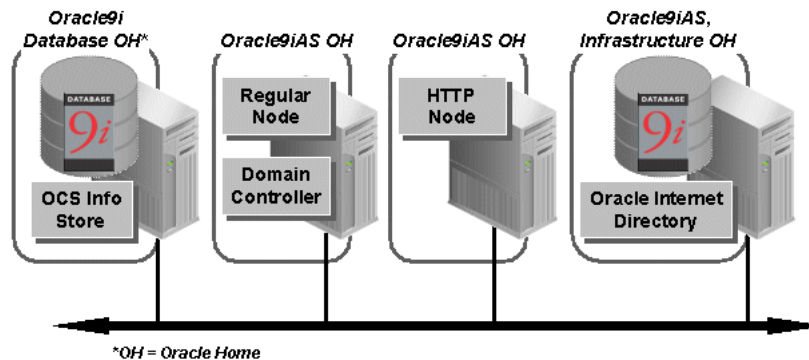
- The regular node supports protocol servers, such as AFP, FTP, NFS, and SMB, as well as agents, such as the Garbage Collection Agent.
- Each regular node is monitored by a node guardian process, which automatically attempts recovery when error conditions occur. This means that the regular node has built-in fault tolerance.
- The HTTP node supports the Oracle Files application, portlet, Oracle FileSync, and WebDAV by means of servlets that are configured to work with the Oracle*9i*AS Containers for J2EE (OC4J).
- The HTTP node's OC4J process is guarded by Oracle Process Management and Notification (OPMN). OPMN will restart the OC4J process if it is stopped unexpectedly.
- The node manager is the actual process that gets started when the node is started. It is responsible for starting the default services and servers for this node. It also provides an administrative API for the node that allows you to find out information about node log levels, locale information, available free memory, and the node's Oracle home.

**Figure 1–2 Oracle Files Nodes**



The Oracle Files domain controller process, node processes, and the database itself can be physically configured on a single host, as shown in [Figure 1–3](#), or across several, separate hosts, as shown in [Figure 1–4](#).

For information about hardware requirements and sizing guidelines for Oracle Files, see the *Oracle Files Planning Guide*.

**Figure 1–3 A Single-Computer Oracle Files Deployment****Figure 1–4 A Multiple-Computer Oracle Files Deployment**

If you choose the single-computer configuration illustrated in [Figure 1–3](#), you must ensure that your host meets the recommended hardware requirements for all components. Be aware that administration is more complex in a single-computer environment. In most cases, you should install Oracle Internet Directory on a separate computer, as shown in [Figure 1–4](#).

With appropriate network load balancers and computer configuration, users may not be aware of whether the Oracle Files instance is running on one host or across several hosts. Users access content, such as folders and documents, using the appropriate client application for a particular Oracle Files protocol server. See the *Oracle Collaboration Suite Release Notes* for specific client certifications.

Windows users can take advantage of Oracle FileSync, a file synchronization client program that lets you work offline (in disconnected mode) and then synchronize file changes with a remote Oracle Files server. See ["Installing Oracle FileSync"](#) on page 2-2 for more information.

When end users connect to a specific protocol server, the underlying service on the node manages authentication of each end user by means of the associated Oracle Internet Directory credential manager, and manages the connection to the database where the content is actually stored.

## Services, Servers, and Agents

Each node supports a *service* with specific configuration parameters, such as language, default character set, credential managers, connections to the database, and cache sizes.

The service, in turn, supports the *servers*. Each server is either a protocol server or an agent. The protocol servers listen for requests from clients on a specific Internet Protocol (IP) 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. Each protocol may interact with Oracle Files in a different way. For example, when uploading a file, FTP just inserts the file, while SMB creates a 0-byte file before creating the actual file.

---

**Note:** The NFS, NTFS, and SMB protocols share the limitation that versioned documents are opened in read-only mode and cannot be deleted, moved, or renamed. This is because some applications, including Microsoft Office applications, save files by first saving the data to a temporary file, deleting the original file, and then renaming the temporary file to the original name. If a document is versioned, this will result in the loss of previous versions.

---

*Agents* perform operations periodically (time-based) or in response to events generated by other Oracle Files servers or processes (event-based). For example, the Content Garbage Collection Agent deletes content no longer associated with any document in Oracle Files. It does so based on an activation period parameter that you set for the server configuration object. See [Appendix C, "Server Configuration Properties"](#) for more information.

Although different agents can run in different nodes, each agent must run only on a single node. Typically, all the shipped agents must be run to ensure a stable system.

The Oracle Files architecture is flexible: services and servers are de-coupled so that you can configure services, protocol servers, and agents across a wide array of hardware to best meet your business needs. 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.

By default, a single service starts on each node, and that service supports all protocol servers selected during installation.

Given the flexibility and granularity of the deployment options, it is important to think about the physical configuration before you install and configure the system. You should plan how the various processes that comprise the system—the domain controller, nodes, agents, and so on—will be configured across your hardware.

The Oracle Files Configuration Assistant sets up an initial domain and node configuration for you, but you can change this later. You can configure the protocol servers at any point by using the Oracle Enterprise Manager Web site.

See [Appendix B, "Service Configuration Reference"](#) for more information about viewing or modifying service configuration parameters.

## Oracle Internet Directory

An Oracle Files service handles user authentication by means of a credential manager. A user's credentials authenticate the user to the system being accessed (for example,

any one of the Oracle Files protocol servers). The credential manager associated with the service tells the service where and how to obtain the credential.

Oracle Files uses Oracle Internet Directory for its identity management directory (in other words, for its list of users and passwords). During configuration of Oracle Files, you use the Oracle Files Configuration Assistant to select an Oracle Internet Directory server to be used with Oracle Files.

When an Oracle Internet Directory credential manager is created during installation, it is created with these default characteristics:

- Ability to accept the following credentials for authentication:
  - Cleartext
  - SMB Challenge/Response
  - HTTP Digest
  - Token
- Protocols that only support Cleartext authentication (AFP, FTP) use the Oracle Files-specific password, rather than the default Oracle Internet Directory password, for enhanced security. Other protocols use the default Oracle Internet Directory password, also known as the Single Sign-On password.

To administer the Oracle Internet Directory associated with Oracle Files, use Oracle Directory Manager and other associated Oracle Internet Directory management tools. See the *Oracle Internet Directory Administrator's Guide* for more information.

## The Subscriber Model

In Oracle Files, a Subscriber is an organizational entity whose users collaborate. Oracle Files Subscribers are based on Oracle Internet Directory Subscribers. The Site Administrator chooses which Subscriber to associate with the Oracle Files domain during Oracle Files configuration.

---

---

**Note:** Because you must use Single Sign-On (SSO) for Oracle Files, and because of current SSO limitations, you can have only one Oracle Files Subscriber.

---

---

The Oracle Files Subscriber has a designated Subscriber Administrator to manage quota, specify Subscriber settings, and perform other tasks. See [Chapter 3, "Oracle Files Administrative Roles and Tasks"](#) for more information about the different types of administrators in Oracle Files.

## Oracle Files Features

Oracle Files administrators should be familiar with the following key features:

- [Three Levels of Administration](#)
- [Workspaces](#)
- [File Management](#)
- [Searching](#)
- [Categories](#)
- [Versioning](#)

- [Review Process](#)
- [Trash](#)
- [Edit-in-Place](#)
- [File Synchronization](#)

## Three Levels of Administration

There are three different administrative roles in Oracle Files:

- The System Administrator is responsible for managing the Oracle Files domain by starting and stopping the domain controller, nodes, services, and servers, and tuning the system to ensure reliability and performance.
- The Site Administrator is responsible for creating, modifying, and deleting Subscribers, as well as registering custom workflows.
- The Subscriber Administrator is responsible for managing quotas, specifying Subscriber settings, administering users, restoring files from the Archive, and administering categories.

Each administrative role does not have to be filled by a different person. In some cases, a single user may act in multiple roles. In addition, each role has a different set of access permissions. See [Chapter 3, "Oracle Files Administrative Roles and Tasks"](#) for more information about the different types of administrators in Oracle Files.

## Workspaces

A *workspace* is where a selected group of Oracle Files users store and collaborate on files and folders. The content of a workspace can be viewed and edited only by its members. A workspace includes at least one administrator, and can include participants and viewers.

Unlike the three administrative roles described in the previous section, the role of the Workspace Administrator is not a true Oracle Files administrative role, since any member of a particular Workspace can be assigned the role of Workspace Administrator.

### Workspace Access Levels

- **Workspace Administrator.** The role of the Workspace Administrator is to manage the workspace. The management role includes such functions as adding and removing workspace members, modifying member access, requesting more workspace quota, and specifying the visibility and workspace type. The Workspace Administrator has full access to the files and folders of the workspace, and can unlock files that have been locked by other workspace members.
- **Participant.** A workspace participant can edit the contents and properties of files and folders in the workspace. A workspace participant can copy and move items to and from the workspace, and can delete files and folders from the workspace, and the workspace's Trash folder.
- **Viewer.** A workspace viewer is restricted to viewing workspace files and folders.

### Workspace Quota

Each workspace is allocated a quota. The contents of each workspace, including its Public folder and Trash folder, count against the workspace's allocated quota. Exceeding the workspace's quota prevents the workspace members from storing

additional content into the workspace. The workspace's administrators can, however, request that the Subscriber Administrator increase the workspace's quota.

See "Workspace Management" in the online help for Oracle Files for detailed information.

## File Management

Each user has a Public folder where he or she can store files, viewable by all users in the Subscriber.

Each user has a Private folder where only he or she can access, store, and view files.

See "File Management" in the online help for Oracle Files for detailed information.

## Searching

Users can conduct simple or advanced searches. Advanced searching lets users refine and combine search criteria.

See "Search Options" in the online help for Oracle Files for detailed information.

---

---

**Note:** In addition to the Oracle Files search feature, Oracle Collaboration Suite users can take advantage of Oracle Collaboration Suite Search, an application that lets users search any and all configured applications in the Oracle Collaboration Suite. See "[Oracle Collaboration Suite Search Configuration](#)" on page 6-17 for more information.

---

---

## Categories

By associating categories with files or folders and modifying the attributes of a category, users can organize and classify their information. Users can also search for files by category.

See "Categories" in the online help for Oracle Files for detailed information.

## Versioning

Users can retain a history of file modifications by creating and saving one or more snapshots of a file.

See "Versioning" in the online help for Oracle Files for detailed information.

## Review Process

Users can submit files for review to a specified set of reviewers. These reviewers fall into two categories: Approvers, who can approve or reject the file, or simply Reviewers, who have read-only access to the file.

The backbone of a review process in Oracle Files is Oracle Workflow. Using a review process, any workspace member can submit for review one or more files from their workspace to other members of their workspace. A review process ends in the approval or rejection of these files, or the process can expire or be canceled. Members can either be Approvers or Reviewers of a review process:

- **Approver.** After receiving notification from Oracle Workflow that he or she has been asked to approve one or more files, an Approver must either approve or reject the files that have been submitted for review. An Approver cannot approve



or reject individual files associated with one review process, but must approve or reject the files as a whole. The workspace member, who initiated the review process, is notified of its approval or rejection.

- **Reviewer.** After receiving notification from Oracle Workflow that he or she has been asked to review one or more files, a Reviewer can review the files. He or she can neither approve or reject files that have been submitted for review.

See "Review Processes and Workflow" in the online help for Oracle Files for detailed information.

### Custom Review Processes

You can create custom review processes, also called workflow processes, to use in Oracle Files. A *workflow designer*, a person with the necessary skills to design a workflow process in Oracle Workflow Builder, creates the custom workflow process. Then, the Site Administrator registers the custom workflow process with Oracle Files.

See "Using Custom Workflows in Oracle Files" in [Chapter 10](#) for detailed information.

## Trash

Files deleted in Private and Public folders are moved to Personal Trash. Files deleted in workspaces are moved to a corresponding Trash folder. A user can request that the Subscriber Administrator restore files that have been emptied from their trash, or from the trash of Workspaces in which they collaborate.

See "File Management" in the online help for Oracle Files for detailed information.

## Edit-in-Place

Using Microsoft Web Folders, Windows users can open and edit an Oracle Files workspace file and save their changes directly back to Oracle Files. When a user opens a workspace file from Microsoft Web Folders to edit in Microsoft Office, the file is automatically locked in Oracle Files. Any changes made to the file are automatically saved back to Oracle Files. When the user closes the file in Microsoft Office, the file is automatically unlocked in Oracle Files.

See "File Management" in the online help for Oracle Files for detailed information.

## File Synchronization

Oracle FileSync synchronizes all file changes between a local computer and Oracle Files, ensuring that the contents of selected local folders and remote folders match.

See "[Oracle FileSync Client Software](#)" on page 2-2 for information about how to install Oracle FileSync. Consult the online help for Oracle FileSync for information about how to synchronize your files.

## Integration with Key Oracle Technologies

Oracle Files, a part of the Oracle Collaboration Suite, is middle-tier software that leverages the capabilities of both Oracle9i Database Server and Oracle9i Application Server.

## Integration With Oracle Collaboration Suite

Oracle Collaboration Suite is an integrated suite of enterprise information management products. It provides a number of shared, “cross-product” features such as an integrated portal home page, a consistent web UI look-and-feel, and federated search for content across all products.

## Integration with Oracle9i Database Server

Oracle Files uses the database to store all content and metadata.

### Oracle9i Database and the Oracle Files Schema

All content and metadata about the Oracle Files 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 the fully functioning system.

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

User content—word processing files, spreadsheets, sound files, presentations, and all manner of other business content—is stored by Oracle Files in the database as LOBs (large objects).

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

### Oracle Text

Oracle Text is full-text retrieval technology built into the Oracle9i Database Server for indexing and searching text and documents stored in the Oracle database. Oracle Text supports mixed languages and character sets in the same index. Oracle Files uses the text indexing and retrieval features of Oracle Text.

### Oracle Advanced Queueing

Oracle Advanced Queueing provides an infrastructure for distributed applications to communicate asynchronously using messages. Oracle Advanced Queueing is built into the Oracle9i Database Server.

See ["Using Custom Workflows in Oracle Files"](#) on page 10-4 for information on how Oracle Files uses Oracle Advanced Queueing to integrate with Oracle Workflow.

### Oracle9i Real Application Clusters (RAC)

A *cluster* is a group of servers that can be used as a single computing system, effectively taking advantage of the combined resources (memory and CPUs) of all the database servers in your cluster.

In a traditional single-server configuration, if the database server goes down due to a hardware, software, or power failure, the Oracle database instance is not available; the single database server has many points of failure.

With Oracle9i Real Application Clusters, if one of the servers in your cluster fails, users are automatically connected to a remaining live server. This failover operation can occur rapidly, since your shared database is already up and running on the other servers in your cluster, effectively masking server failures from your users.

Consult your database documentation for more information about setting up Oracle9i Real Application Clusters. See [Appendix D, "Setting Up Oracle Files With RAC"](#) for more information about setting up Oracle Files for use with RAC.

## Integration with Oracle9i Application Server

Oracle Files is designed to integrate with several important components from the Oracle9i Application Server product family, including Oracle Internet Directory, the Oracle Enterprise Manager Web site, and Oracle9iAS Containers for J2EE (OC4J).

See the *Oracle Collaboration Suite Installation and Configuration Guide* for detailed information on recommended Oracle Files installation and deployment models.

### Oracle9iAS Containers for J2EE (OC4J)

Oracle9iAS Containers for J2EE (OC4J) is a J2EE-compliant application server that supports Java Server Pages (JSP), Java servlets, Enterprise Java Beans, 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 .WAR (Web Application Archive), .EAR (Enterprise Application Archive), and .JAR (Java Archive) files. Oracle Files uses the Java Servlet and the runtime environment of OC4J to support the HTTP/DAV servlet, application servlet, and portlet servlet.

OC4J is automatically configured for the Oracle Files HTTP node as part of the Oracle Files configuration process. You can manage OC4J through the Oracle Enterprise Manager Web site.

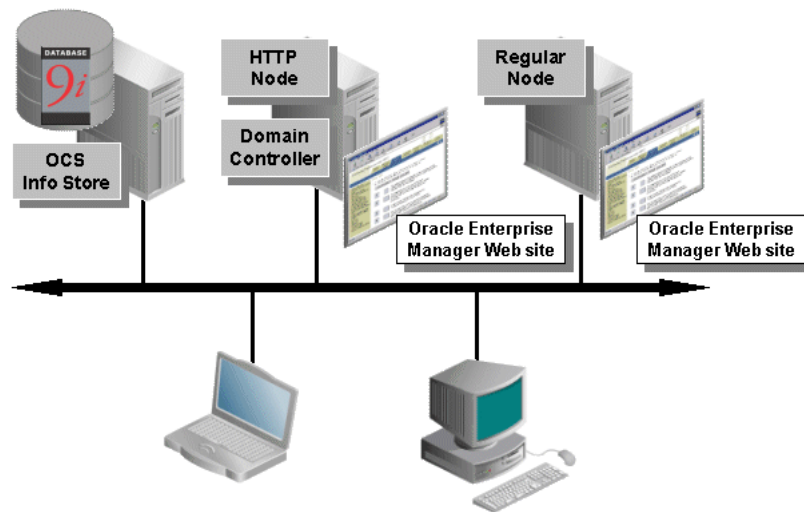
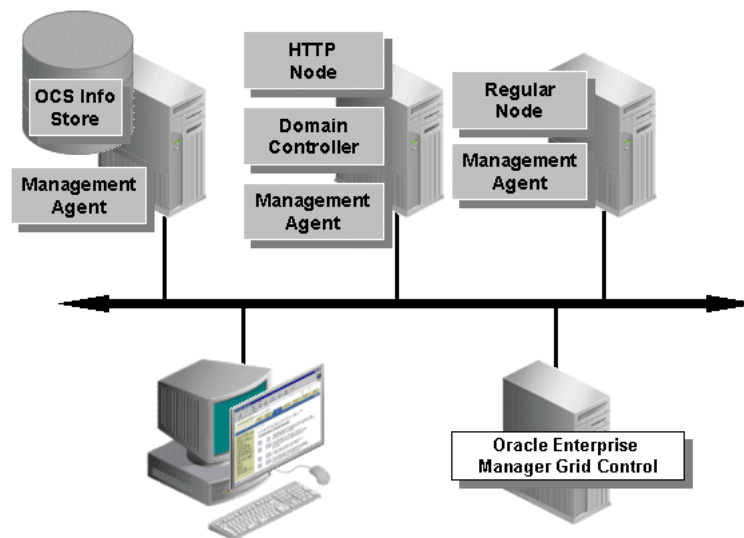
### Oracle Enterprise Manager

Oracle Enterprise Manager is a systems management software application that enables you to manage and monitor Oracle9i Application Server instances and other Oracle server products. Oracle Enterprise Manager has two separate Web-based interfaces: the Oracle Enterprise Manager Web site and the Grid Control. The Oracle Enterprise Manager Web site is used to connect to a single middle-tier host, while the Grid Control provides centralized management for multiple middle tiers, including Oracle9iAS middle tiers, Oracle9iAS Infrastructure tiers, and Oracle9i Database Server hosts. Refer to [Figure 1-5](#) and [Figure 1-6](#) for diagrams of the Oracle Enterprise Manager Web site and the Grid Control.

---

**Note:** 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 the Oracle Files middle tier in its own Oracle home. For more information, refer to *Oracle Enterprise Manager Managing Oracle Collaboration Suite* on Oracle Technology Network at: <http://otn.oracle.com>

---

**Figure 1–5 Oracle Enterprise Manager Web site****Figure 1–6 Oracle Enterprise Manager 10g Grid Control**

Oracle Files uses the Oracle Enterprise Manager Web site to operate and monitor system processes associated with the Oracle Files domain and nodes. The Grid Control is used for access to Oracle Files 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.

Using a Web browser from anywhere on the network, you can connect to the Oracle Enterprise Manager Web site, from which you can launch the domain controller process, start and stop nodes, and monitor the domain and nodes.

The first page you see when you access the Oracle Enterprise Manager Web site is the Oracle9i Application Server Farm Home page, which lets you view a set of related application server instances associated with the same Oracle9i Application Server Infrastructure tier.

## Oracle Internet Directory

Oracle Internet Directory is Oracle's LDAP (Lightweight Directory Access Protocol) v.3-compliant directory service implementation. Oracle Internet Directory provides user authentication and other directory service features, like user provisioning, to Oracle Collaboration Suite components.

For more information about Oracle9i Application Server and its components, see the *Oracle9i Application Server Installation Guide*, *Oracle Internet Directory Administrator's Guide*, and *Oracle Enterprise Manager Concepts*.

## Oracle Workflow

Oracle Workflow is business-process automation software. Oracle Workflow lets you automate the process of routing and approving information, according to business rules you specify. Key components include:

- Oracle Workflow Builder, a modeling tool that lets you define and model your business processes in a graphical environment
- Workflow Engine, which coordinates the routing activities and approvals at runtime
- A notifications system for sending notifications to and receiving notifications from users (such as approvers) in a workflow
- A Web-based graphical monitoring tool for tracking workflow processes

Oracle Files comes with a default workflow process (also called review process) that enables Oracle Files users to submit their documents for review. In addition, a *workflow designer*, a person with the necessary skills to design a workflow process in Oracle Workflow Builder, can create custom workflow processes for Oracle Files. Once a custom workflow process has been created, the Site Administrator is responsible for registering it with Oracle Files.

See ["Using Custom Workflows in Oracle Files"](#) in [Chapter 10](#) for more information about custom workflows.



---

## Oracle Files Protocol Support

This chapter discusses the protocol servers supported by Oracle Files, along with the client access paths and software for the supported protocols. Topics include:

- [Industry-Standard Protocol Servers](#)
- [Client Software and Access Paths](#)
- [Using Oracle Files with NFS](#)

### Industry-Standard Protocol Servers

Oracle Files supports a wide range of protocols, including the following:

- HTTP, the Hypertext Transfer Protocol, is used for Web browser-based access. HTTP has been extended with WebDAV, a protocol 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.
- FTP, the File Transfer Protocol, is used for file transfers across Wide Area Networks such as the Internet.
- SMB, the Server Message Block protocol, lets you map Oracle Files as a network drive or browse to it through the Network Neighborhood.

---

**Note:** SMB protocol support is provided by the Oracle Files SMB server when Oracle Files is running on UNIX or Linux. When Oracle Files is running on Windows, SMB protocol support is provided by the Oracle Files NTFS server, due to the differing architectures of Windows versus UNIX.

---

- AFP, the AppleTalk Filing Protocol, enables Macintosh users to use Oracle Files as if it were an AppleShare server. Mac OS X supports AFP over TCP, which allows AFP services to be made available over the Internet and networks that use TCP/IP as the underlying transport.
- NFS, the Network File System, is a mechanism for mounting remote file systems on UNIX platforms.

Users can connect to Oracle Files using protocols appropriate to their platform. For example, Macintosh users can connect to Oracle Files as if it were an AppleShare server, Windows users can map a network drive or connect using Web Folders, and UNIX clients can connect using NFS.

Some protocols, such as FTP and AFP, send unencrypted passwords over the network. Oracle Internet Directory users should use an Oracle Files-specific password for these protocols for greater security. See ["Oracle Files-Specific Passwords"](#) on page 8-2 for more information.

## Client Software and Access Paths

This section describes how to install the Oracle FileSync client software. It also provides information about the client access paths for various protocols, including AFP, HTTP, and NFS.

For complete client certification information, see the Oracle Files chapter of the *Oracle Collaboration Suite Release Notes*.

### Oracle FileSync Client Software

In addition to using the networking protocols or client applications native to the Windows operating system, Windows users can install and use Oracle FileSync to keep local directories on a desktop computer and folders in Oracle Files synchronized.

#### Installing Oracle FileSync

Oracle FileSync is client software for Windows that enables users to keep files synchronized between their local computer and Oracle Files.

Follow these steps to install Oracle FileSync:

1. Save and exit all Windows applications.
2. Log in to Oracle Files and click **Help**. On the main online help page, click the link in the Oracle FileSync section.
3. Save the install executable to your hard drive.
4. Double-click `fileSync.exe` to run the installation program.
5. Follow the instructions and accept the defaults. The application will be installed on the Windows client computer in the following directory:  
`c:\Program Files\Oracle\Oracle FileSync`
6. To start the Oracle FileSync application, select **Oracle FileSync** from the Windows **Start > Programs** menu.

See the Oracle FileSync online help for information about using Oracle FileSync.

### Client Access Paths

With an account name and password, users—administrators or regular end-users—can access Oracle Files using the client tool of their choice. Web users can use a Web browser for HTTP access. Windows users can map drives or use WebDAV, and Macintosh users can use the **Go** menu to access the AFP server. [Table 2-1](#) lists some of the client platforms, protocols, and access methods supported by Oracle Files. See the Oracle Files chapter of the *Oracle Collaboration Suite Release Notes* for complete client certification information.



**Table 2–1 Client Platforms and Protocol Support**

Client Platform	Protocols Supported	Access Using
Windows	FTP, HTTP, SMB/NTFS, WebDAV, NFS	Browser, Windows Explorer, Oracle FileSync, Hummingbird Maestro
Macintosh (Mac OS 10.2)	AFP, FTP, HTTP	Macintosh <b>Go</b> Menu (Mac OS X), Browser
UNIX	FTP, NFS	Command line
Red Hat Linux Adv. Server 2.1 (Kernel 2.4.9-e.16)	FTP, NFS	mount command

---

**Note:** 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 hostname.

---

The following sections provide additional information about client access to Oracle Files:

- [AppleTalk Filing Protocol \(AFP\) Access for Macintosh Clients](#)
- [HTTP \(Web Browser\) and WebDAV Access](#)
- [SMB/NTFS Access](#)
- [FTP Access](#)
- [NFS \(Network File System\) Protocol Access](#)

### AppleTalk Filing Protocol (AFP) Access for Macintosh Clients

Oracle Files includes an AFP 2.2-compliant AppleTalk Filing Protocol (AFP) server. A Mac OS X client can use the AFP Server just as if it were an AppleShare server. The steps required to connect to the AFP server depend on the Mac OS on the client. Mac OS X clients use the **Go** menu from the desktop.

The Chooser does not exist in Mac OS X. Clients should connect using the new **Go** menu, as follows:

1. Select **Go** from the menu.
2. Select **Connect to Server**. A dialog box appears.
3. Enter the address of the Oracle Files middle-tier computer running the AFP Server in URL format:

```
afp://computer_name
```

The AppleShare icon appears on the client desktop.

### HTTP (Web Browser) and WebDAV Access

Use the following URL to access Oracle Files with HTTP, WebDAV, and Oracle FileSync:

```
http://server_name:7777/files/content
```

The port number for Oracle Files varies depending on whether Oracle9iAS Web Cache is configured. If Oracle9iAS Web Cache is not configured, the value is typically 7778.

The URL is required for access from:

- Web browser
- DAV applications, such as Web Folders
- Oracle FileSync utility

### **SMB/NTFS Access**

SMB, the Server Message Block protocol, lets you map Oracle Files as a network drive or browse to it through the Network Neighborhood.

The Oracle Files server provides SMB protocol support when Oracle Files is running on UNIX or Linux. When Oracle Files is running on Windows, SMB protocol support is provided by the Oracle Files NTFS server, due to the differing architectures of Windows versus UNIX.

The following restrictions apply to SMB/NTFS access:

- Use the syntax `\\servername\myhome` or `\\servername\allpublic` to map a directory.
- Use an existing Oracle Files user name and password when connecting.
- You cannot have multiple SMB/NTFS mappings as different users to folders on the same server. This is a limitation of the Windows operating system.
- Versioned documents cannot be deleted, moved, or renamed over SMB/NTFS.

### **FTP Access**

FTP, the File Transfer Protocol, is used for file transfers across Wide Area Networks such as the Internet.

The most lightweight protocol, FTP can move large amounts of data faster than the other protocols. For bulk operations, such as migrating from an existing system, FTP is the protocol of choice. You need to use either command line FTP or a GUI FTP client for this step.

To FTP your files into Oracle Files, the following requirements must be met:

- An FTP client must be installed on your local computer.
- You must know the port number for FTP, which was specified during Oracle Files configuration.

### **NFS (Network File System) Protocol Access**

Oracle Files provides an NFS protocol server that is certified for use with several NFS clients, including:

- Solaris 2.8 and Solaris 2.9
- Red Hat Linux Adv. Server 2.1 (Kernel 2.4.9-e.16)
- Windows NT and 2000 Clients using Hummingbird Maestro NFS

If the Oracle Files NFS server is configured as the primary NFS server, then UNIX clients (Solaris 2.8, Solaris 2.9, and Red Hat Linux Adv. Server 2.1) can access the server using the standard NFS mount command, as shown in [Table 2-2](#).

**Table 2–2 Mount NFS Server (Configured as Primary NFS Server)**

Syntax	Example
<code>mount host:/ mount_point</code>	<code>mount ifsserver:/ /data/ifs</code>

If the Oracle Files NFS server is configured as the secondary NFS server, or if the Oracle Files NFS server is not on the standard port number, Solaris clients must specify the `public` option and Linux clients must specify the mount port, as described in ["Solaris 2.8 and Solaris 2.9 Clients"](#) on page 2-5 and ["Red Hat Linux Adv. Server 2.1 and Red Hat Linux 8.0 Clients"](#) on page 2-6.

Other caveats apply to Hummingbird Maestro clients, as detailed in ["Linking an NFS Directory Using the NFS Maestro Network Access Tool"](#) on page 2-6.

**NFS Server Limitations** Permission mode bits used by native UNIX NFS are not used by the Oracle Files NFS protocol server. Instead, as it does with other protocol servers, Oracle Files NFS uses access control lists (ACLs) to control access.

---

**Note:** If Oracle Files is configured to use a schema that is enabled for multiple subscribers, the guest user cannot access any folders using NFS. The guest account is valid only in a dedicated single-subscriber schema.

---

In addition, the Oracle Files NFS server does not support the following:

- UNIX symbolic and hard links
- UNIX `chown`, `chgrp`, and `chmod` commands
- UNIX lock manager
  - Handles returned by the Oracle Files NFS server are not compatible with the UNIX lock manager. Applications requiring UNIX lock manager services do not work with the Oracle Files NFS server.

NFS clients cannot access the checked-out version of a versioned document. To avoid potential conflicts, the Oracle Files NFS server does not allow access by NFS clients to the checked-out version of a versioned document. In addition, versioned documents cannot be deleted, moved, or renamed.

**Solaris 2.8 and Solaris 2.9 Clients** If the Oracle Files NFS server is running as the primary NFS server on the host, users can enter the standard mount command as shown in [Table 2–2](#). If the Oracle Files NFS server is the secondary NFS server on the host, you must explicitly include the port number in the mount command:

```
mount nfs://host:port/ mount_point
```

For example:

```
mount nfs://ifsserver:4049/ /data/ifs
```

Alternatively, you can use the following command:

```
mount -o port=port,public host:/ mount_point
```

For example:

```
mount -o port=4049,public ifsserver:/ /data/ifs
```

**Red Hat Linux Adv. Server 2.1 and Red Hat Linux 8.0 Clients** If the Oracle Files NFS server is running as the primary NFS server on the host, users can enter the standard mount command as shown in [Table 2–2](#). If the Oracle Files NFS server is the secondary NFS server on the host, you must explicitly include the port number in the mount command:

```
mount -o port=port,mountport=portno1 host:/ mount_point
```

For example:

```
mount -o port=4049,mountport=4048 ifsserver:/ /data/ifs
```

**Windows Clients** While client access to NFS is available on all UNIX operating systems, Windows systems require additional client software. Hummingbird Maestro NFS is a Windows client certified for use with Oracle Files NFS Server.

- Windows 2000 users who want to connect to Oracle Files NFS Server must use Hummingbird Maestro NFS 7.0.
- Windows NT users who want to connect to Oracle Files NFS Server can use Hummingbird Maestro NFS 6.0 or later.

See the *Oracle Collaboration Suite Release Notes* for other supported NFS client applications and version numbers.

---

---

**Note:** Enter the fully-qualified hostname (for example, `hostname.yourcompany.com`) in the Windows client network configuration for the NFS client. Move the NFS client to the top of the list (network access in Network control panel, if you have more than one NFS client installed) to ensure that its driver is used for the connection.

---

---

**Linking an NFS Directory Using the NFS Maestro Network Access Tool** Before using the Hummingbird NFS Maestro client to access the Oracle Files NFS server, check that the NFS Maestro client is properly configured.

1. From the NFS Maestro folder, start the NFS Network Access tool. The NFS Network Access dialog appears.
2. Enter the host name of the Oracle Files NFS server in the Network Path field using the following format:  
`\\hostname\`
3. In the Authentication Details area, enter the UNIX user name and password for accessing the Oracle Files NFS server. Select **System/UNIX Authentication** as the Authentication Protocol.
4. Set the following Miscellaneous values:
  - **DOS-style sharing:** Deselect DOS-style file sharing unless you have the HCLNFSD daemon running on the NFS server computer. HCLNFSD is required for DOS-style file sharing. If the HCLNFSD daemon is not running on the NFS server, response times in accessing files will be unacceptable.
  - **UNIX lock manager:** Deselect UNIX lock manager if it is checked. The Oracle Files NFS server is not compatible with the UNIX lock manager.
  - **CD-ROM:** Deselect this box if it is selected. This is used for CD-ROM or other read-only file systems.

5. Click **Advanced** to display the Advanced Connection Properties dialog.
6. Select **Preserve Case for Filename Case**.
7. If the Oracle Files NFS server is running as a secondary NFS server, change the value of **NFS Port number** from the standard port (2049) to the alternate port number that the Oracle Files NFS server is using.
8. To use TCP instead of UDP for connection to the NFS server, select **Use TCP**.  
TCP uses the standard NFS port 2049. Do not select this box if the Oracle Files NFS server is running on an alternate port.

**Linking an NFS Directory Using the Command Line** If the Oracle Files NFS server is the primary NFS server on the host, you can mount Oracle Files using the following Maestro command-line syntax:

```
nfs link drive: \\host\ username
```

For example:

```
nfs link n: \\ifsserver\ scott
```

If the Oracle Files NFS server is the secondary NFS server on the host, you must specify the Oracle Files NFS server port number in the command line:

```
nfs link drive: \\host\ username /n:port
```

For example:

```
nfs link n: \\ifsserver\ scott /n:4049
```

The `nfs link` command uses the default values configured for the NFS Maestro Client, unless you specify options listed in [Table 2–3](#).

**Table 2–3 Maestro Command-Line Options**

Option	Meaning	Usage Note
/L:s	Use DOS-style sharing.	Requires that the HCLNFSD daemon run on the server.
/L:	Disables locking.	Use this parameter if the server does not have the HCLNFSD daemon running.
/M:p	Preserve case of file names.	N/A
/A:u	Use System/UNIX authentication.	Always use this setting.
/T	Use a TCP connection instead of a UDP connection (optional).	TCP connections always use port 2049. Do not use this option unless the Oracle Files NFS server is running port 2049 (the default).

Problems are often caused by incorrect port numbers. If the HCLNFSD daemon is not running on the server, then DOS-style locking and sharing must be disabled on the client.

**Maestro Error Messages** [Table 2–4](#) lists some common error messages and other Maestro client problems.

**Table 2–4 Maestro Client or Server Error Messages or Problem Symptoms**

Problem	Corrective Action
"Access denied by server" message	Check that the correct port number is being used for the Oracle Files NFS server.  A TCP connection will always use the standard NFS port (2049). Do not use this option if the Oracle Files NFS server is running on an alternate port.
"Authorization Error" message	The user name and password are invalid. Specify a UNIX user name and password that are valid on the authentication server.
"Bad Network Name" message	Verify that the host name and path name are specified correctly. If they are, then use the NFS Maestro <code>Rpcinfo</code> tool and verify that the NFS server (process number 100003) is running on the host.
Maestro client appears to hang	Verify that the <code>HCLNFSD</code> daemon is running on the server computer. If it is not, either start the daemon (if possible), or verify that <b>DOS-style sharing</b> and <b>UNIX lock manager</b> have been deselected in the Maestro client settings.  For the Maestro command line, specify the <code>/L:</code> command-line option when linking to disable locking. You can check all current mapped drives by using Maestro's <code>nfs use</code> command.
"Network Timeout or HCLNFSD/PCNFSD not running on Host" message	Verify that the default authentication server has been correctly configured in the NFS client. Verify that the <code>HCLNFSD</code> daemon is running. Perform the verifications listed for the <a href="#">"Bad Network Name" message</a> .
<code>nfs link</code> command hangs	Verify that the correct host name and port number are specified and that the Oracle Files NFS server is running.
"NFS service not responding" error message	Verify that the correct host name and port number are specified and that the Oracle Files NFS server is running.
"Permission denied" error message	Verify that the host name and path name are specified correctly. Verify that the port is correctly specified for the Oracle Files NFS server.

## Using Oracle Files with NFS

Depending on the specifics of your Oracle Files deployment, you may choose to perform the post-configuration task of configuring the NFS Server. This task is not required to get Oracle Files up and running.

### Configuring the NFS Server

You can make the following three configuration changes to the Oracle Files NFS Protocol Server:

- [Mapping UNIX UIDs to Oracle Files User Accounts](#). Creates a mapping between UNIX UIDs and Oracle Files user accounts so that users can access Oracle Files after logging on to their UNIX user accounts.
- [Setting Up a Trusted Client List](#). Explicitly grants or revokes access privileges to a specific IP address, host computer, or domain. The Trusted Client list is an Oracle-specific capability to enhance NFS protocol security.

- **Enabling NIS Authentication.** If your environment uses NIS for user, group, and password information, you can configure the Oracle Files NFS protocol server to use NIS to authenticate users.

In most environments, you should map the UNIX and Oracle Files accounts. The user account map is a domain property, and it can be updated dynamically. You do not need to restart the server to have the mappings take effect. In addition, the changes are persistent, even after the server is restarted.

The Trusted Client List and NIS authentication are NFS server configuration properties.

### Mapping UNIX UIDs to Oracle Files User Accounts

The Oracle Files NFS Protocol Server uses the UNIX system authentication process to authenticate users. The UNIX UID (user identification) number is passed to the Oracle Files NFS protocol server.

If their UNIX accounts are mapped to Oracle Files accounts, users can log in to the UNIX operating system and access Oracle Files without having to undergo an additional login process.

UNIX-UID-to-Oracle Files client mapping is configured in the `IFS.DOMAIN.PROTOCOL.NFS.UidToUserMap` domain property. You can map UIDs manually, through the Oracle Enterprise Manager Web site, or you can upload UIDs using the Java Bulk NFS Tool.

**Mapping UIDs Manually** To map UIDs manually using the Oracle Enterprise Manager Web site:

1. From the Oracle9iAS Farm Home page, click the name of the application server on which Oracle Files is running. The Oracle9iAS Instance Home page appears, listing all the components running on the application server instance. The Oracle Files domain appears in the following format:

```
ifs_db_host:port:db_service:files_schema
```

2. Click the name of the Oracle Files domain. The Oracle Files home page appears, listing the Domain Controller and nodes that comprise the domain.
3. Click **Domain Properties** (under the Configuration heading). The Domain Properties page appears, listing 25 property bundles at a time. Scroll down until you find `IFS.DOMAIN.PROTOCOL.NFS.UidToUserMap`. The property might be located on a second or subsequent page.
4. Click **IFS.DOMAIN.PROTOCOL.NFS.UidToUserMap**. The Edit page appears. By default, the UID 60001 (the default UNIX guest account) is listed on the page.
5. Click **Add** to add a UNIX UID and create a mapping to an Oracle Files user account:
  - Enter the UID in the **Name** field.
  - Enter the Oracle Files user account name in the **Value** field.
  - Leave the **Type** setting as **String**.
6. Continue adding users in this manner until you have added all users with UNIX client accounts that will access Oracle Files using NFS.

**Mapping UIDs Using the Bulk NFS Tool** To map UIDs using the Bulk NFS Tool:

1. On any middle-tier host, ensure that the CLASSPATH includes `files.jar`.  
This file is located in the `$ORACLE_HOME/ifs/files/lib` directory.
2. Run the following single line with the required values:  

```
java oracle.ifs.protocols.nfs.tools.UidLoader SmallServiceConfiguration system  
files_system_user_password uidfile=UidToName
```

Where `UidToName` is the full path to a flat file you have created with entries of type:

```
files_user:x:uid_on_client
```

For example:

```
jsmith:x:44610
```
3. When prompted, enter the name of the Oracle Files domain, in the format:  

```
ifs://db_host:port:db_service:files_schema
```
4. When prompted, enter the Oracle Files schema password.

### Setting Up a Trusted Client List

You can use Oracle Enterprise Manager Web site to create a list of trusted clients for Oracle Files to enhance security. Oracle recommends that you change these settings in the Configuration Object and then load the server on the service using the modified configuration object so that the client list is used after a restart. Optionally, you can modify these properties dynamically.

1. From the Oracle9iAS Farm Home page, click the name of the application server on which Oracle Files is running. The Oracle9iAS Instance Home page appears, listing all the components running on the application server instance. The Oracle Files domain appears in the following format:  

```
ifs_db_host:port:db_service:files_schema
```
2. Click the name of the Oracle Files domain. The Oracle Files Home page appears, listing the domain controller and nodes that comprise the domain.
3. Click **Server Configurations** (under the Configuration heading). The Server Configurations page appears, listing 25 property bundles at a time. Scroll down until you find `NfsServerConfiguration`.
4. Click **NfsServerConfiguration**. The Edit page appears.
5. Scroll down to the Properties section of the page to the `IFS.SERVER.PROTOCOL.NFS.TrustedClientList` and the `IFS.SERVER.PROTOCOL.NFS.TrustedClientsEnabled` properties. The properties might be located on a second or subsequent page.
6. Select **IFS.SERVER.PROTOCOL.NFS.TrustedClientsEnabled** and click **Edit**. The Edit Property page appears.
7. Set the **Value** to **True**. Click **OK** to save the change and return to the Edit `NfsServerConfiguration` page.
8. Select **IFS.SERVER.PROTOCOL.NFS.TrustedClientList** and click **Edit**. Specify each entry in one of the following formats:
  - **Client address:** Specify a hostname or an IP address. For example, `smith.oracle.com` or `130.35.59.9`.



- **Domain suffix:** Specify the domain as a string starting with a period character. For example, `.us.oracle.com`.
- **Subnet:** Specify the subnet as an at symbol (@) character followed by an IP address, with an optional subnet bit length (/n) specifying the number of significant bits in the subnet address. You can omit low order zero bytes of the subnet address. For example, `@130.35.68.0`, `@130.35.68` or `@130.35.68.0/24`.

If an entry is preceded by a hyphen, then that specific client will be denied access through the Oracle Files NFS server.

9. Click **OK** to save the change and return to the Edit NfsServerConfiguration page.
10. Click **OK** to save and return to the Server Configuration page.

If the node is currently running, you must either restart the node or load the modified configuration object onto the node.

To reload the node configuration:

1. Return to the Oracle Files Home page.
2. Click the Node where the NFS protocol server (NfsServer) is running. The Node page appears.
3. Stop the existing NfsServer (if one is already running on the service).
4. Unload this NfsServer.
5. Load the modified NFS protocol server object.
6. Start the new, modified NfsServer.
7. Restart the service.

### Enabling NIS Authentication

NIS (Network Information System) is a centralized management facility that consolidates UNIX password, group, and host file information. It is a distributed database of information that is easier to maintain than individual files (`/etc/group`, `/etc/passwd`, `/etc/hosts`) in large UNIX networks.

To enable NIS authentication using the Oracle Enterprise Manager Web site:

1. From the Oracle9iAS Farm Home page, click the name of the application server on which Oracle Files is running. The Oracle9iAS Instance Home page appears, listing all the components running on the application server instance. The Oracle Files domain appears in the following format:  
`iFS_db_host:port:db_service:files_schema`
2. Click the name of the Oracle Files domain. The Oracle Files Home page appears, listing the domain controller and nodes that comprise the domain.
3. Click **Server Configurations** (under the Configuration heading). The Server Configurations page appears, listing 25 property bundles at a time. Scroll down until you find NfsServerConfiguration.
4. Click **NfsServerConfiguration**. The Edit page appears.
5. Scroll down to the Properties section of the page to the `IFS.SERVER.PROTOCOL.NFS.NISEnabled` and `IFS.SERVER.PROTOCOL.NFS.NISServiceProvider` properties.

6. Select **IFS.SERVER.PROTOCOL.NFS.NISEnabled** and click **Edit**. The Edit Property page appears.
7. Set the **Value** to **True**. Click **OK** to save the change and return to the Edit NfsServerConfiguration page.
8. Select **IFS.SERVER.PROTOCOL.NFS.NISServiceProvider** and click **Edit**.
9. Specify the name of the NIS server in your network that should be used to authenticate users. The format is:  
  
`nis://NIS_server_name/files_domain`
10. Click **OK** to save the change and return to the Edit NfsServerConfiguration page.
11. Click **OK** to save and return to the Server Configuration page.

If the node is currently running, you must either restart the node or load the modified configuration object onto the node.

To restart the node:

1. Return to the Oracle Files Home page.
2. Select the node where the NFS protocol server is running and click **Stop**.
3. On the Warning page, click **Yes** to stop the node. The status of the node changes to Down.
4. Select the node and click **Start**. The status of the node changes to Up.

---

## Oracle Files Administrative Roles and Tasks

---

There are three administrative roles in Oracle Files: System Administrator, Site Administrator, and Subscriber Administrator. Each type of administrator performs different tasks, using tools specifically for the task at hand.

This chapter provides an overview of the Oracle Files administrative roles and their associated tasks. Topics include:

- [Administrative Roles Quick Reference](#)
- [System Administrator](#)
- [Site Administrator](#)
- [Subscriber Administrator](#)

### Administrative Roles Quick Reference

[Table 3–1](#) summarizes the documentation resources for each administrative role.

**Table 3–1 Administrative Roles Quick Reference**

If you are a:	Your responsibilities include:	Consult these sources:
System Administrator	<ul style="list-style-type: none"><li>■ Installing and configuring Oracle Files</li><li>■ Managing the Oracle Files domain, nodes, services, and servers</li></ul>	<i>Oracle Files Planning Guide</i> <i>Oracle Collaboration Suite Installation and Configuration Guide</i> <i>Oracle Collaboration Suite Release Notes</i> <a href="#">Chapter 3, "Oracle Files Administrative Roles and Tasks"</a> <a href="#">Chapter 4, "Administration Tools Overview"</a> <a href="#">Chapter 5, "Managing the Oracle Files Domain"</a> <a href="#">Chapter 6, "Changing Configuration Settings"</a> <a href="#">Chapter 7, "Monitoring Domain, Node, and Service Performance"</a> <a href="#">Chapter 8, "Oracle Files Security"</a> <a href="#">Chapter 9, "Maintenance and Tuning"</a> <a href="#">Chapter 10, "Customizing Oracle Files"</a> <a href="#">Chapter 11, "Troubleshooting"</a>

**Table 3–1 (Cont.) Administrative Roles Quick Reference**

If you are a:	Your responsibilities include:	Consult these sources:
Site Administrator	<ul style="list-style-type: none"> <li>Adding, deleting, and managing subscribers</li> <li>Registering custom workflows</li> </ul>	<a href="#">Chapter 3, "Oracle Files Administrative Roles and Tasks"</a> <a href="#">Chapter 4, "Administration Tools Overview"</a> <a href="#">Chapter 10, "Customizing Oracle Files"</a> "Site Administration" in the Oracle Files online help
Subscriber Administrator	<ul style="list-style-type: none"> <li>Managing users, quotas, categories, subscriber settings, and content</li> </ul>	<a href="#">Chapter 3, "Oracle Files Administrative Roles and Tasks"</a> <a href="#">Chapter 4, "Administration Tools Overview"</a> "Subscriber Administration" in the Oracle Files online help

## Administrative Accounts

The following table summarizes the administrative accounts used in Oracle Files and other related applications:

**Table 3–2 Administrative Accounts**

Account Name	Password	Purpose
system	Set during Oracle Files configuration.	Used internally. If you run <code>ifscs</code> to add a second OCS middle tier for an additional HTTP node, regular node, or to migrate the domain controller, and you choose to reuse the existing files schema, you will need the <code>system</code> account. When you connect to Oracle Enterprise Manager Web site on the new middle tier, you will be prompted to enter the system user name and password. You also need the <code>system</code> account to run the Bulk NFS Tool; see <a href="#">"Using Oracle Files with NFS"</a> on page 2-8 for more information.
ias_admin	Set during OCS Infrastructure or OCS middle tier installation.	Used to access Oracle Enterprise Manager Web site.
cn=orcladmin	Set during OCS Infrastructure installation.	Used for Oracle Internet Directory administration. Also used in the Oracle Files Configuration Assistant when you create the files schema.
site_admin	Set during Oracle Files configuration.	Used to access Site Administration functions in the Oracle Files Web interface. Also needed to run the bulk tools.
Subscriber Administrator account (user-defined)	Site Administrators choose the Subscriber Administrator user name when they create the Subscriber. The password is auto-generated and e-mailed to the Subscriber Administrator.	Used to access Subscriber Administration functions in the Oracle Files Web interface. Also needed to run the bulk tools.

## System Administrator

The System Administrator installs and configures Oracle Files, manages the Oracle Files domain, and performs system tuning and troubleshooting. Most of these tasks are the subject of a chapter in this guide.

**Table 3–3 System Administrator Task Reference**

Task:	Consult:
Installation and configuration	<a href="#">Oracle Files Planning Guide</a> <a href="#">Oracle Collaboration Suite Installation and Configuration Guide</a> <a href="#">Oracle Collaboration Suite Release Notes</a> <a href="#">Chapter 4, "Administration Tools Overview"</a> <a href="#">Chapter 8, "Oracle Files Security"</a> <a href="#">Chapter 10, "Customizing Oracle Files"</a>
Domain management, configuration and monitoring	<a href="#">Chapter 1, "Oracle Files Concepts"</a> <a href="#">Chapter 4, "Administration Tools Overview"</a> <a href="#">Chapter 5, "Managing the Oracle Files Domain"</a> <a href="#">Chapter 6, "Changing Configuration Settings"</a> <a href="#">Chapter 7, "Monitoring Domain, Node, and Service Performance"</a>
System tuning	<a href="#">Chapter 9, "Maintenance and Tuning"</a>
Troubleshooting	<a href="#">Chapter 11, "Troubleshooting"</a>
Reference	<a href="#">Appendix A, "Oracle Text Reference"</a> <a href="#">Appendix B, "Service Configuration Reference"</a> <a href="#">Appendix C, "Server Configuration Properties"</a> <a href="#">Appendix D, "Setting Up Oracle Files With RAC"</a> <a href="#">Appendix E, "Migrating Data to Oracle Files"</a> <a href="#">Appendix F, "FTP Quote Command Reference"</a> <a href="#">Appendix G, "Globalization Support"</a>

The Oracle Enterprise Manager Web site provides access to basic Oracle Files process management and monitoring functions, such as starting and stopping the domain, nodes, services, and servers. This tool also allows administrators to monitor and dynamically tune the domain's nodes, services, and servers.

After installing and initially configuring Oracle Files, you can monitor document storage, session usage, and memory usage so you can adjust service and server parameters to maintain optimum performance. For example:

- You can use the Server Configurations page to create a new server.
- You can use the Domain Performance and Statistics pages to monitor the domain and obtain an overall usage summary for the domain.
- If the storage space consumed by users is approaching the quota allocated, you can add storage or reduce the number of documents stored.

## Skills Required to Administer Oracle Files

System administrators should have the following skills:

- **Basic Oracle RDBMS administration experience.** Since the file system is stored in an Oracle9i database, you need to understand the basics of how to administer the database.
- **Knowledge of Internet and Intranet protocols.** You need to understand how HTTP, SMB, WebDAV, and the other networking protocols work.
- **Familiarity with Internet technologies.** Since Oracle Files serves Web pages representing the file system, relies on XML for system configuration data, and uses Java as the language of server-side application development, familiarity with these technologies is important.
- **Web Server administration experience.** You need to understand how to administer the Oracle HTTP Server.

## Site Administrator

The Site Administrator manages Oracle Files Subscribers. A Subscriber is a discrete organizational entity whose users can collaborate on files and folders. Users in one Subscriber do not have access to the content of users in another Subscriber. The Site Administrator creates, modifies, and deletes Subscribers.

---

**Note:** Because Site Administrators must use Single Sign-On (SSO) for Oracle Files, and because of current SSO limitations, you can have only one Oracle Files Subscriber.

---

The Site Administrator has a different view in Oracle Files than regular users:

**Figure 3–1 Site Administration View**

ORACLE Collaboration Suite  
Files

Logout Workflow Preferences Help

Site Administration

Subscribers Defaults Workflow

You are logged in as: site\_admin

### Browse Subscribers

New Subscriber

☒ Indicates that the Subscriber is disabled.  
☒ Indicates that the OiD subscriber is no longer configured for OiD. None of the subscriber's users will be able to log in.

Select and ... Email Administrator Enable Disable Delete

Select All | Select None

Select Subscriber	Allocated Quota	Consumed Quota	Allocated Users	Users Created
<input type="checkbox"/> Oracle	25 GB	3.2 MB	30	30
<input type="checkbox"/> us	35 GB	14.9 MB	70	9

New Subscriber

Site Administration | Logout | Workflow | Preferences | Help

Copyright © 2001, 2003 Oracle. All rights reserved.

Subscribers are created through Oracle Files integration with Oracle Internet Directory. The System Administrator selects the Oracle Files Subscriber from Oracle Internet Directory during Oracle Files installation.

The Site Administrator and the Subscriber Administrator log in to Oracle Files through the Administration Login page. This page can be found at:

<http://host:port/files/app/AdminLogin>

## Managing Subscribers

The primary role of the Site Administrator is to manage the Oracle Files Subscriber. The following sections provide an overview of the primary tasks involved in managing the Subscriber.

See "Site Administration" in the online help for Oracle Files for detailed information.

### Creating, Modifying, and Deleting Subscribers

After the Oracle Files Configuration Assistant is used to create a new Oracle Files domain, you can configure Oracle Internet Directory Subscribers for Oracle Files so that they may be created in Oracle Files.

In addition, since the use of Single Sign-On is expected, only the default Subscriber should be created in Oracle Files.

---

**Note:** If you change the default Subscriber, you must restart the Oracle Files domain. See ["Starting and Stopping the Oracle Files Domain"](#) on page 5-2 for more information.

---

### Enabling and Disabling Subscribers

Using the Oracle Files wizards, the Site Administrator can enable or disable a Subscriber.

See ["Subscriber Administrator"](#) for more information about Subscribers.

### Specifying Notification and Archive Settings

The Site Administrator can specify notification and archive settings, such as setting up a notification that warns of a Subscriber's expiration date, or specifying how long archived files should remain in the Archive.

### E-mailing a Subscriber

The Site Administrator can e-mail a Subscriber Administrator. The Site Administrator, for instance, may want to contact a Subscriber Administrator about a Subscriber's expiration date.

### Viewing Subscriber Statistics

The Subscriber Statistics page in Oracle Files is divided into two sections: Subscriber Information and User and Workspace Information. Both sections provide statistical information about their respective areas; for instance, the total space consumed by the Subscriber and the total space consumed by Workspaces.

### Resetting a Subscriber Administrator Password

The Site Administrator can reset a Subscriber Administrator's password.

## Registering Custom Workflows

A *workflow designer*, a person with the necessary skills to design a workflow process in Oracle Workflow Builder, can create a custom workflow process for Oracle Files. Once the custom workflow process has been created, the Site Administrator is responsible for registering it with Oracle Files.

See ["Registering a Custom Workflow with Oracle Files"](#) in [Chapter 10](#) for more information about registering custom workflows.

## Subscriber Administrator

In Oracle Files, a Subscriber is an organizational entity whose users can collaborate on files and folders. Each Subscriber has its own Subscriber Administrator. The Subscriber Administrator, an enhanced user, administers the Subscriber by managing quota, users, and categories, specifying Subscriber settings, and restoring files from the Archive. The Subscriber Administration has a different view in Oracle Files than regular users:

**Figure 3–2 Subscriber Administration View**



See "Subscriber Administration" in the online help for Oracle Files for detailed information.

The Site Administrator and the Subscriber Administrator log in to Oracle Files through the Administration Login page. This page can be found at:

`http://host:port/files/app/AdminLogin`

## Setting Defaults

One of the critical roles of the Subscriber Administrator is to specify default settings for users. The following list summarizes tasks regarding default settings.

See "Subscriber Administration" in the online help for Oracle Files for detailed information.

### Specifying Default User Settings

The Subscriber Administrator can specify default settings for all Subscriber users, such as whether their Public folder should by default be enabled or disabled.

### Specifying Notification Settings

The Subscriber Administrator can specify the number of days prior to a user's expiration date that the Subscriber Administrator is notified of the user's expiration.



**Specifying Default Quota Settings**

The Subscriber Administrator can specify the default quota of each new user and Workspace.

**Specifying Default Public Folder Settings**

The Subscriber Administrator can specify user and Workspace folder settings, such as whether the Public folder is enabled or disabled.

**Specifying Default Language Settings**

The Subscriber Administrator can specify the default display language, document language, document character set, and time zone of a Subscriber.

**Subscriber Information Tasks**

Oracle Files provides two mechanisms for information: Subscriber statistics and communication with the Site Administrator.

See "Subscriber Administration" in the online help for Oracle Files for detailed information.

**Viewing Subscriber Statistics**

The Subscriber Administrator can view detailed information about the Subscriber.

**Requesting to Modify Subscriber's Settings**

The Subscriber Administrator can submit a request to the Site Administrator to extend or modify a Subscriber's settings. For example, the Subscriber Administrator can request to increase the Subscriber quota.

**Contacting the Site Administrator**

The Subscriber Administrator can e-mail the Site Administrator regarding Subscriber-related issues.

**User Management Tasks**

The Subscriber Administrator manages users in the Subscriber by performing tasks such as creating users or updating user quota.

See "Subscriber Administration" in the online help for Oracle Files for detailed information.

**Creating and Provisioning Users**

Oracle Files users must be created in Oracle Internet Directory, using the Oracle Directory Manager administration tool. Since Oracle Directory Manager runs as a servlet in the OC4J\_DAS instance, you must start the OC4J\_DAS instance on the Infrastructure host in order to access Oracle Directory Manager.

After users have been created, and after the Site Administrator has created the Oracle Files Subscriber, users are automatically provisioned in Oracle Files every 15 minutes by the FilesOidUserSynchronizationAgent.

You can change the default provisioning time period by changing the `IFS.SERVER.TIMER.ActivationPeriod` parameter of the `FilesOidUserSynchronizationAgent`. You can choose a time period anywhere

from 5 minutes to 24 hours. See ["Changing a Server Configuration"](#) on page 6-15 for information about editing servers and agents.

Additionally, once a user has been created in Oracle Internet Directory, logging in to Oracle Files as that user will immediately provision the user in Oracle Files, irrespective of the time interval specified for the Agent (this is a new feature in Oracle Collaboration Suite Release 2).

As a result of the provisioning process, Oracle Files users receive an e-mail confirming that they have an account on Oracle Files, with a URL to the Oracle Files login page and instructions on how to enable protocol access to Oracle Files.

**Creating Users in Oracle Internet Directory** In order for users to access Oracle Files, they must first be created as users in Oracle Internet Directory.

To create users in Oracle Internet Directory:

1. Make sure that the OC4J\_DAS instance has been started on the Infrastructure host.
2. Using a Web browser, connect to the Infrastructure host by entering:

```
http://fully_qualified_hostname:7777/oiddas
```

3. Log in as the Oracle Internet Directory Administrator (typically `cn=orcladmin`).
4. Click the **Directory** tab.
5. Click **Create**.

The Create User page appears.

6. Fill in the fields.
7. Click **Submit**.

---

---

**Caution:** User names may not contain spaces or any of the following characters: `& ' % ? \ / + = ( ) * ^ , ; | ' ~`

---

---

Although Oracle Files supports multibyte character sets, some protocols, such as WebDAV, do not support multibyte user names. For this reason, when you create users for Oracle Files in Oracle Internet Directory, you should create the names using single-byte characters only. Users whose names are created with multibyte characters will be unable to access content through some of the Oracle Files protocol servers.

Similarly, you should create user passwords in ASCII since some protocols, such as SMB, only accept ASCII passwords. Users whose passwords are created with non-ASCII characters will be unable to access content through some of the Oracle Files protocol servers.

For more information about creating users in Oracle Internet Directory, see the *Oracle Internet Directory Administrator's Guide*.

## E-mailing Users

The Subscriber Administrator can e-mail users in his or her Subscriber.

## Modifying User Information

A User Information page exists for each user in the Subscriber, where the Subscriber Administrator can modify the user's information and settings.

### **Updating User Quota**

The Subscriber Administrator can grant users quota increases upon request.

### **Enabling and Disabling Users**

The Subscriber Administrator can enable and disable users. Disabled users cannot access Oracle Files; enabled users can access Oracle Files.

### **Deleting Users**

The Subscriber Administrator can delete any user who has been deleted from Oracle Internet Directory, but only one at a time, and only when the user is unsubscribed from all Workspaces. When the Subscriber Administrator deletes a user, the items in the user's Private and Public folders appear in the Archive.

## **Category Management Tasks**

The Subscriber Administrator is responsible for managing *categories*. Categories are a way for users to classify and manage content. When implemented and associated with content, categories can be used as search criteria.

See "Subscriber Administration" in the online help for Oracle Files for detailed information.

### **Creating Categories**

The Subscriber Administrator can create categories using the category creation wizard.

### **Modifying Categories**

The Subscriber Administrator can modify existing categories using the category modification wizard. Category attributes cannot be modified; the Subscriber Administrator must delete the attribute and then create a new attribute.

### **Deleting Categories**

The Subscriber Administrator can delete categories using the category deletion wizard. When the Subscriber Administrator deletes a category, any file or folder associated with it loses this association.

## **Trash Management Tasks**

Trash is a collection deleted files and folders. Subscriber Administrators can view, copy, move, delete, and empty the contents of Trash generated by users and by Workspaces.

See "Subscriber Administration" in the online help for Oracle Files for detailed information.

## **Archival File and Folder Management Tasks**

Files and folders that are deleted from Trash are moved to the Archive. The Subscriber Administrator is responsible for handling file archival functions, such as restoring deleted files and folders.

See "Subscriber Administration" in the online help for Oracle Files for detailed information.

### **Recovering a File at a User's Request**

The Subscriber Administrator can restore a file or folder, deleted from Trash, at the e-mail request of a user.

### **Restoring a File or Folder from the Archive**

The Subscriber Administrator can restore four types of items that users empty or delete from Trash:

- Deleted files and folders of active users.
- Deleted files and folders of active Workspaces.
- Deleted files and folders of deleted users.
- Deleted files and folders of deleted Workspaces.

## **Workspace and File Management Tasks**

The Subscriber Administrator is able to access Workspaces in the Subscriber to administer and to take advantage of the content management capabilities of Oracle Files.

See "Subscriber Administration" in the online help for Oracle Files for detailed information.

### **Working with Workspaces**

Although the Subscriber Administrator cannot be a member of a Workspace, as an enhanced user the Subscriber Administrator has full administrative access to the files and folders in every Workspace.

### **Updating Workspace Quota**

The Subscriber Administrator can update Workspace quotas in response to a Workspace Administrator's e-mail requests.

### **Locking and Unlocking Files**

A Subscriber Administrator can lock and unlock files in any Workspace.

---

## Administration Tools Overview

A full range of administration tools are provided with Oracle Files, including configuration wizards, management tools, and scripts. Using these administration tools, you can:

- Configure Oracle Files
- Start and stop domains and nodes
- Manage service and server objects
- Work from the command line
- Migrate data and users to Oracle Files
- Monitor domain, service, and node performance

This chapter provides an overview of the different administration tools. Topics include:

- [Oracle Files Configuration Assistant](#)
- [Management Tools](#)
- [Scripts](#)
- [Bulk Administration Tools for Oracle Files](#)

### Oracle Files Configuration Assistant

The Oracle Files Configuration Assistant is an installation and configuration wizard that lets you create an Oracle Files domain and specify an Oracle Internet Directory credential manager to associate with the domain. The wizard also lets you upgrade an existing Oracle Files instance to a newer release.

The Configuration Assistant is specific for the release of Oracle Files. Use this tool to:

- Set up the domain controller to run on the local host.
- Set up the nodes to run on the local host.
- Select which protocol servers you want to run on the local host.
- Create an Oracle Files schema and all associated objects in the Oracle database.
- Select an Oracle Internet Directory credential manager.
- Add middle tiers to the domain.

The primary purpose of the Oracle Files Configuration Assistant is to set up the initial configuration of your system. If you want to modify the initial configuration after installation, use the Oracle Enterprise Manager Web site.

See the *Oracle Collaboration Suite Installation and Configuration Guide* for full instructions on how to use the Oracle Files Configuration Assistant.

## Running the Oracle Files Configuration Assistant

You can launch the Oracle Files Configuration Assistant from the command line by executing the `ifscsca` script, located in the following directory:

```
$ORACLE_HOME/ifs/files/bin
```

To run `ifscsca`, you must be logged on as the OS user who installed and configured all other Oracle software on that middle-tier host (probably `oracle`).

You can also prepare or modify a response file and pass the filename to the Oracle Files Configuration Assistant as a parameter, for a non-interactive, or "silent," configuration. See the *Oracle Collaboration Suite Installation and Configuration Guide* for details.

## Management Tools

Which management tool you use will depend on the function to be performed, and whether you want to work with the Oracle Files domain as one of several middle-tier applications integrated with Oracle Enterprise Manager:

- [Oracle Enterprise Manager Web Site](#)
- [Oracle Enterprise Manager 10g Grid Control](#)
- [Administration Tabs in Oracle Files](#)
- [Oracle Directory Manager](#)

## Oracle Enterprise Manager Web Site

Oracle Enterprise Manager Web site is a Web-based management tool designed specifically for Oracle9i Application Server. You can monitor and configure the components of your Oracle9iAS installations, as well as configure and manage the Oracle Files domain and nodes. It also allows administrators to monitor and dynamically tune the domain's nodes, services, and servers.

Using Oracle Enterprise Manager Web site, you can:

- Start and stop the domain, nodes, services, protocol servers, and agents using a Web browser from any computer on the network.
- Configure protocol servers, agents, nodes, services, and change settings dynamically, for the current runtime session; change settings permanently; and change default settings to be used as the basis for new servers.
- Display runtime operational data and charts about the domain, nodes, hosts, and servers at runtime, so you can monitor performance and change system configuration, if necessary.

You can use a command-line tool, `emctl`, to perform Oracle Enterprise Manager tasks such as starting and stopping the Oracle Enterprise Manager process. See the *Oracle9i Application Server Administrator's Guide* for complete information.

## Using the Oracle Enterprise Manager Web Site to Manage Oracle Files

The following sections describe how to start the Oracle Enterprise Manager process, access the Oracle Enterprise Manager Web site, and navigate to the Oracle Files Home page.

**Starting the Oracle Enterprise Manager Process** If it is not running already, start the Oracle Enterprise Manager process by executing its startup script from the command line (UNIX) or by starting the corresponding service (Windows), as shown in [Table 4–1](#). In order to control the Oracle Files domain and the nodes using the Oracle Enterprise Manager Web site, the Oracle Enterprise Manager process must be running on each host that comprises the domain.

**Table 4–1 Starting and Stopping the Oracle Enterprise Manager Process**

Operation	UNIX-based Hosts	Windows Hosts
Starting the Oracle Enterprise Manager process	<code>\$ORACLE_HOME/bin/emctl start</code>	Start the Windows service for Oracle Enterprise Manager.
Stopping the Oracle Enterprise Manager Process	<code>\$ORACLE_HOME/bin/emctl stop</code>	Stop the Windows service for Oracle Enterprise Manager.

**Accessing the Oracle Enterprise Manager Web Site** Follow these steps to connect to the Oracle Enterprise Manager Web site:

1. From a Web browser, access the following URL:

`http://host_name:port`

The value for *host\_name* is the name of the Oracle Files middle tier you want to manage. The value for *port* is typically 1810.

2. Log in as *ias\_admin*, using the password you specified during Oracle9iAS installation.

The Oracle9iAS Farm Home page appears, listing the set of application server instances that use the Infrastructure Services of the same Oracle9iAS Infrastructure tier.

**Accessing the Oracle Files Home Page** Follow these steps to navigate to the Oracle Files Home page in the Oracle Enterprise Manager Web site:

1. From the Oracle9iAS Farm Home page, click the name of the application server on which Oracle Files is running.

The Oracle9iAS Instance Home page appears, listing all the components running on the application server instance. The Oracle Files domain appears in the following format:

`iFS_db_host:port:db_service:files_schema`

After initial Oracle Files configuration, you must restart the Oracle Enterprise Manager process (see [Table 4–1](#) on page 4-3). If you access the Oracle Enterprise Manager Web site after configuration without restarting the Oracle Enterprise Manager process, the Oracle Files domain link will not be active.

2. Click the name of the Oracle Files domain. The Oracle Files home page appears, listing the Domain Controller and nodes that comprise the domain.

Under certain conditions, such as after an upgrade, you will be prompted to enter the Oracle Files system user name and password when you navigate to the Oracle Files Home page in the Oracle Enterprise Manager Web site. If you see this prompt, you must provide the system user name and password in order to see elements of the Oracle Files domain from the Oracle Files Home page in the Oracle Enterprise Manager Web site. The system password was set when you configured Oracle Files.

You can avoid this behavior by manually encrypting the system password in `targets.xml`. See ["Encrypting the System Password in targets.xml"](#) on page 8-7 for more information.

## Oracle Enterprise Manager 10g Grid Control

The Oracle Enterprise Manager 10g Grid Control is a Web-based tool that provides centralized management for multiple middle tiers, including Oracle9iAS middle tiers, Oracle9iAS Infrastructure tiers, and Oracle9i Database Server hosts. If the Grid Control has been installed and configured, Oracle Files can use the Grid Control for access to metric data, such as document statistics, node statistics, and users, as well as to monitor alerts that have been defined for some metrics.

The Grid Control manages each host through the Oracle Management Agent installed on each middle-tier host. An Oracle Management Agent must be installed in its own Oracle home on a middle-tier host in order for that middle tier to be managed by the Grid Control. See *Oracle Enterprise Manager Basic Installation and Configuration* for information about installing the Grid Control.

Metric collection for Oracle Files is not set up automatically. You must configure Oracle Enterprise Manager to manage Oracle Files. For details on how to do this, see *Oracle Enterprise Manager Managing Oracle Collaboration Suite* on the Oracle Technology Network at:

<http://otn.oracle.com>

### Accessing the Grid Control

You can access the Grid Control from a Web browser.

1. Use the following URL to access the Grid Control:

`http://grid_control_host_name:port/em`

---

**Note:** If the Oracle Management Service is running in non-secure mode, access the Grid Control using the Web Cache port. Using the Web Cache port is a prerequisite for self-monitoring. The default port is assigned in the range of 7777-7877. For example:

`http://testcomputer.us.oracle.com:7777/em`

If the Management Service is running in secure mode, access the Grid Control over HTTPS. The default port is assigned in the range of 4443-4543. For example:

`https://testcomputer.us.oracle.com:4443/em`

---

2. Log in as `sysman`, using the password you specified during Oracle Enterprise Manager installation. Or, log in as another Grid Control user with administrator privileges.

See ["Viewing Oracle Files Metrics in the Grid Control"](#) on page 7-7 for information about accessing Oracle Files metrics.



## Administration Tabs in Oracle Files

When you log in to Oracle Files as either a Site or Subscriber Administrator, you can see the administration tabs in the Oracle Files Web interface. The Site Administrator and the Subscriber Administrator log in to Oracle Files through the Administration Login page. This page can be found at:

`http://host_name:port/files/app/AdminLogin`

See "Site Administration" and "Subscriber Administration" in the Online Help for Oracle Files for detailed information about administrative operations in the Oracle Files Web interface.

## Oracle Directory Manager

Oracle Directory Manager is the administrative tool for Oracle Internet Directory.

See the *Oracle Internet Directory Administrator's Guide* for more information about Oracle Directory Manager.

## Scripts

Oracle Files scripts are listed in [Table 4-2](#). To run these scripts, you must be logged on as the OS user who installed and configured all other Oracle software on that middle-tier host (probably `oracle`). In addition, some functions in the `ifsctl` script must be performed by the OS root user.

All Oracle Files scripts are located in the following directory:

`$ORACLE_HOME/ifs/files/bin/`

**Table 4-2 Oracle Files Scripts**

Script Name	Description
<code>ifsca</code>	Runs the Oracle Files Configuration Assistant.
<code>ifsctl</code>	Starts, stops, and monitors Oracle Files domains and nodes. See <a href="#">"Managing the Oracle Files Domain from the Command Line"</a> on page 5-8 for more information.
<code>ifsbulkadmintools</code>	Runs the Bulk Administration tools.

There are a variety of Oracle9i Application Server scripts and command-line tools that you will need in order to manage your system. Two of the most important tools, `emctl` and `opmnctl`, are listed in [Table 4-3](#). For a full list of Oracle9iAS scripts, see the *Oracle9i Application Server Administrator's Guide*.

**Table 4-3 Important Oracle9i Application Server Scripts**

Script Name	Location	Description
<code>emctl</code>	<code>\$ORACLE_HOME/bin/</code>	Manages Oracle Enterprise Manager.
<code>opmnctl</code>	<code>\$ORACLE_HOME/opmn/bin/</code>	Manages Oracle Process Management and Notification Server. Used to start and stop OC4J processes and the Oracle HTTP Server.
<code>dcmctl</code>	<code>\$ORACLE_HOME/dcm/bin</code>	Provides a command-line alternative for some Oracle9iAS management tasks. Used to retrieve status information about Oracle Files HTTP nodes.

## Bulk Administration Tools for Oracle Files

A Subscriber Administrator can use the Bulk Administration tools to manage users and Workspaces in Oracle Files.

Each tool works in a similar manner: it reads an XML file containing a list of "actions" (such as creating a workspace or updating users), processes the list, and executes the actions.

The Bulk Administration tools include:

- [User Administration Tool](#)
- [Workspace Administration Tool](#)

## Running the Bulk Administration Tools

To run the Bulk Administration tools, the Subscriber Administrator must run the `ifsbulkadmintools` script, located in the following directory:

```
$ORACLE_HOME/ifs/files/bin/
```

When you run the Bulk Administration tools, the following parameters must be specified in the following order:

1. The type of tool you want to use:
  - **users** for the User Administration Tool
  - **workspaces** for the Workspace Administration Tool
2. An Oracle Files Domain. For example:  
`ifs://user-sun.us.company.com:1521:seamus:ifuser`
3. The default service configuration name (for example, `SmallServiceConfiguration`). This value is specified in the following domain property:  
`IFS.DOMAIN.LIBRARYOBJECT.SERVICECONFIGURATION.DefaultServiceConfiguration`  
See "[Domain Properties](#)" on page 6-1 for more information.
4. The Oracle Files schema password.
5. The Site Administrator user name (`site_admin`).
6. The Site Administrator password.
7. The Subscriber Administrator user name.
8. The Subscriber Administrator password.
9. The name of the XML file defining the list of actions to perform.

**See Also:** "[Administrative Accounts](#)" on page 3-2 for more information about steps 5 - 8

For example, to invoke the User Administration tool, you could enter the following:

```
ifsbulkadmintools users ifs://user-sun.us.company.com:1521:seamus:ifuser  
MediumServiceConfiguration ocsv2 site_admin mgr filessba welcome1 user.xml
```

To invoke the Workspace Administration tool, you could enter the following:

```
ifsbulkadmintools workspaces ifs://user-sun.us.company.com:1521:seamus:ifuser
```

```
MediumServiceConfiguration ocsv2 site_admin mgr filessba welcome1 workspace.xml
```

Log information is printed to the screen.

## User Administration Tool

The User Administration tool updates the profile of each user listed in an XML file that you create, unless the user does not exist in the Subscriber. If the user does not exist in the Subscriber, the User Administration tool skips the entry and prints an error in the log.

---

---

**Note:** You cannot change user passwords with the User Administration tool.

---

---

### Sample XML File

This XML file contains one action for updating users:

```
<?xml version="1.0" encoding="UTF-8" ?>
<users>
  <action label="update">
    <class>oracle.ifs.files.admin.bulk.user.action.UpdateNormalUsersAction
    </class>
    <user>
      <userid>test.user</userid>
      <quota>25</quota>
      <locale>us</locale>
      <publicfolder enabled="yes" />
    </user>
  </action>
</users>
```

For `<locale>`, enter an ISO locale code such as **es**. To see a list of codes, refer to the **Display Language** drop-down list on the General User Preferences page in Oracle Files. In this list, ISO locale codes are displayed in parentheses.

The User Administration tool performs DTD validation. For this reason, your XML file must include the DTD, either inline or referenced externally.

### DTD for the User Administration Tool

```
<!DOCTYPE users [

  <!ELEMENT users (defaults?, (action|condition)+)>

  <!ELEMENT defaults (property+)>

  <!ELEMENT condition (condition|action)+>
  <!ATTLIST condition type NMTOKEN #REQUIRED>
  <!ATTLIST condition op NMTOKEN #REQUIRED>
  <!ATTLIST condition left CDATA #REQUIRED>
  <!ATTLIST condition right CDATA #REQUIRED>

  <!ELEMENT action (class, property*, user+)>
  <!ATTLIST action label ID #REQUIRED>
  <!ATTLIST action description CDATA #IMPLIED>

  <!ELEMENT class (#PCDATA)>
```

```
<!ELEMENT property EMPTY>
<!ATTLIST property name NMTOKEN #REQUIRED>
<!ATTLIST property value CDATA #REQUIRED>

<!ELEMENT user (userid, email?, firstname?, lastname?, quota?, locale?,
publicfolder?)>

<!ELEMENT userid (#PCDATA)>
<!ATTLIST userid enabled (yes|no) #IMPLIED>

<!ELEMENT email (#PCDATA)>

<!ELEMENT firstname (#PCDATA)>

<!ELEMENT lastname (#PCDATA)>

<!ELEMENT quota (#PCDATA)>

<!ELEMENT locale (#PCDATA)>

<!ELEMENT publicfolder EMPTY>
<!ATTLIST publicfolder enabled (yes|no) "yes">
]>
```

### Troubleshooting the User Administration Tool

You should be aware of the following limitations of the User Administration tool:

- **Quota:** The User Administration tool does not update a user's quota should the quota exceed the granted limit. Also, a user's quota is not updated if the new value is below that of the user's consumed storage.
- **Enabling or Disabling Public Folders:** A user's Public Folder that is not empty cannot be disabled.

## Workspace Administration Tool

The Workspace Administration tool creates or updates workspaces listed in an XML file you create. The class of the action specified in the referenced XML file determines which operation is performed. For example, if the class is `CreateWorkspacesAction`, one or more workspaces are created. If the class is `UpdateWorkspacesAction`, one or more workspaces are updated.

### Sample XML File

This XML file contains one action for updating workspaces and another action for creating workspaces:

```
<?xml version="1.0" encoding="UTF-8" ?>
<workspaces>

  <action label="create">
    <class>oracle.ifs.files.admin.bulk.workspace.action.CreateWorkspacesAction
    </class>
    <workspace name="test_workspace" type="public">
      <description>Test Workspace for the administration tool</description>
      <member name="test.user" access="admin" />
    </workspace>
  </action>

  <action label="update">
```

```

<class>oracle.ifs.files.admin.bulk.workspace.action.UpdateWorkspacesAction
</class>
  <workspace name="test_workspace">
    <quota>40</quota>
    <publicfolder enabled="no" />
  </workspace>
</action>

</workspaces>

```

The Workspace Administration tool performs DTD validation. For this reason, your XML file must include the DTD, either inline or referenced externally.

### DTD for the Workspace Administration Tool

```

<!DOCTYPE workspaces [

  <!ELEMENT workspaces (defaults?, (action|condition)+)>

  <!ELEMENT defaults (property+)>

  <!ELEMENT condition (condition|action)+>
  <!ATTLIST condition type NMTOKEN #REQUIRED>
  <!ATTLIST condition op NMTOKEN #REQUIRED>
  <!ATTLIST condition left CDATA #REQUIRED>
  <!ATTLIST condition right CDATA #REQUIRED>

  <!ELEMENT action (class, property*, workspace+)>
  <!ATTLIST action label ID #REQUIRED>
  <!ATTLIST action description CDATA #IMPLIED>

  <!ELEMENT class (#PCDATA)>

  <!ELEMENT property EMPTY>
  <!ATTLIST property name NMTOKEN #REQUIRED>
  <!ATTLIST property value CDATA #REQUIRED>

  <!ELEMENT workspace (description?, quota?, publicfolder?, member*)>
  <!ATTLIST workspace name CDATA #REQUIRED>
  <!ATTLIST workspace type (public|private) #IMPLIED>

  <!ELEMENT description (#PCDATA)>

  <!ELEMENT quota (#PCDATA)>

  <!ELEMENT publicfolder EMPTY>
  <!ATTLIST publicfolder enabled (yes|no) "no">

  <!ELEMENT member EMPTY>
  <!ATTLIST member name CDATA #REQUIRED>
  <!ATTLIST member access (admin|RW|RO|delete) #REQUIRED>
]>

```

Note the following about the Workspace Administration DTD:

- The type attribute of the workspace element defaults to Private if not specified.
- If the quota element is not specified, the quota property setting defaults to the Subscriber's default Workspace quota.

- If the `public_folder` element is not specified, the public folder property setting defaults to Enabled, if the Workspace type is public. Otherwise, it defaults to Disabled.
- The delete value for the `member_access` property is valid only for the `update` action of the Workspace Administration tool.

### Troubleshooting the Workspace Administration Tool

The following sections provide troubleshooting information about creating and updating workspaces using the Workspace Administration tool.

**Troubleshooting Workspace Creation** You should be aware of the following limitations when you create workspaces using the `create` action of the Workspace Administration tool:

- A Workspace name may not already exist in the Subscriber.
- A Workspace name may not contain the following characters: `\ / : * ? " < > |`
- A Workspace Administrator must be specified in the list of members.
- Creation of the Workspace(s) in the Subscriber may not exceed the Subscriber's total quota.
- A Workspace name may not end in a period.

**Troubleshooting Workspace Updating** You should be aware of the following limitations when you update workspaces using the `update` action of the Workspace Administration tool:

- **Quota:** A workspace cannot be updated if the new value causes the Subscriber's total quota to exceed the granted limit, or if the new value is less than the workspace's consumed storage.
- **Public Folder:** A workspace public folder that is not empty cannot be disabled.
- **Members:** A workspace must have at least one Administrator. If not, the Workspace cannot be updated.

---

## Managing the Oracle Files Domain

Use the Oracle Enterprise Manager Web site to perform a variety of domain operations, including starting and stopping the Oracle Files domain, starting and stopping servers, and managing nodes. You can also manage the Oracle Files domain from the command line using `ifscctl` and `opmnctl`.

Topics in this chapter include:

- [About the Oracle Files Domain](#)
- [Starting and Stopping the Oracle Files Domain](#)
- [Migrating the Domain Controller](#)
- [Managing the Node Processes](#)
- [Starting, Stopping, Suspending, and Resuming Servers](#)
- [Managing the Oracle Files Domain from the Command Line](#)
- [Oracle Process Management and Notification](#)

### About the Oracle Files Domain

The *domain controller* manages the set of nodes comprising the domain. The domain controller controls which nodes are running, tracks the status of each node, and allows nodes to be monitored and administered. The Oracle Files software runs as a set of middle-tier processes, called *nodes*. Each node executes on a particular computer, or *host*. Although a domain's nodes are often split across a set of hosts, a single host can have more than one Oracle Files node. Each node has a name, which is unique across the Oracle Files domain. Oracle Files nodes are processes of Oracle Files managing one or more services and servers (agents and protocols).

There are two types of nodes: regular nodes, and HTTP nodes. The Oracle Files HTTP node runs as part of an Oracle9iAS Containers for J2EE (OC4J) process.

The domain controller polls the nodes that are configured to run under its control. Once all the nodes are identified, you will see them under the list of nodes for the specific domain.

In order to control the Oracle Files domain and the nodes using the Oracle Enterprise Manager Web site, the Oracle Enterprise Manager process must be running on each host that comprises the domain. See [Table 4-1](#) on page 4-3 for information about how to start and stop the Oracle Enterprise Manager process.

The fully-qualified name for an Oracle Files domain is:

```
ifs://db_host:port:db_service:files_schema
```

For example:

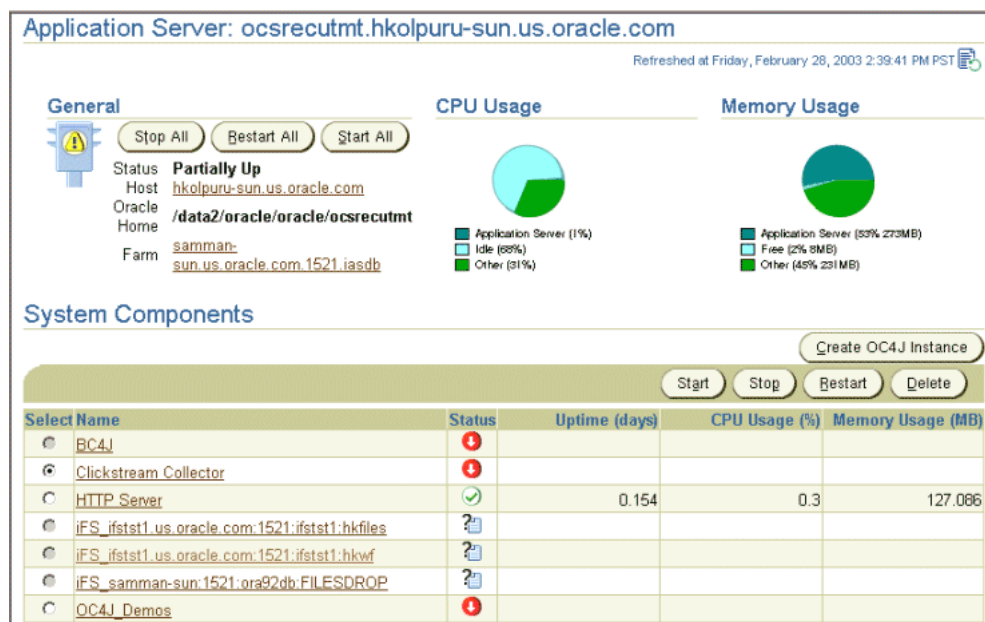
```
ifs://testcomputer.us.oracle.com:1521:filesservice:filesschema
```

## Starting and Stopping the Oracle Files Domain

This section provides instructions for starting and stopping the Oracle Files domain using the Oracle Enterprise Manager Web site.

1. From the Oracle9iAS Farm Home page, click the name of the application server on which Oracle Files is running. The Oracle9iAS Instance Home page appears.

**Figure 5–1 Oracle9iAS Instance Home Page**



Among these components, Oracle Files domain targets appear in the following format:

```
ifs_db_host:port:db_service:files_schema
```

For example:

```
ifs_iftst1.us.oracle.com:1521:iftst1:hkfiles
```

After initial Oracle Files configuration, you must restart the Oracle Enterprise Manager process (see [Table 4–1](#) on page 4-3). If you access the Oracle Enterprise Manager Web site after configuration without restarting the Oracle Enterprise Manager process, the Oracle Files domain link will not be active.

2. From the Oracle9iAS Home page, click the name of the Oracle Files domain you want to manage.

The Oracle Files Home page appears, showing the status of the domain controller and the set of nodes that belong to the domain. A checkmark icon in the Status column means the component has been started.

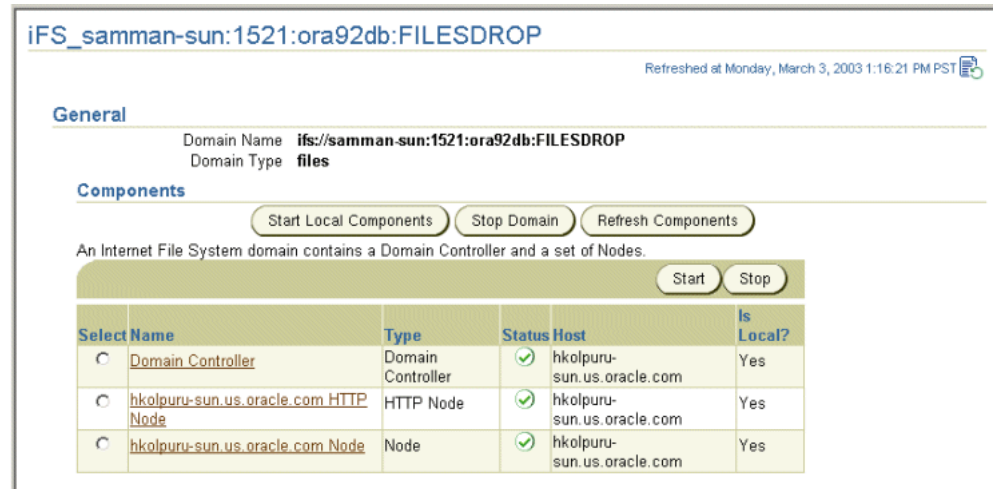
Under certain conditions, such as after an upgrade, you will be prompted to enter the Oracle Files system user name and password when you navigate to the Oracle Files Home page in the Oracle Enterprise Manager Web site. If you see this



prompt, you must provide the system user name and password in order to see elements of the Oracle Files domain from the Oracle Files Home page in the Oracle Enterprise Manager Web site.

You can avoid this behavior by manually encrypting the system password in `targets.xml`. See ["Encrypting the System Password in targets.xml"](#) on page 8-7 for more information.

**Figure 5–2 Oracle Files Home Page**



3. Start, stop, or refresh the domain, as follows. Some operations are performed on local domain components, while others are performed on the entire domain.

- To start all the components on the local middle-tier host, click **Start Local Components**. To start a single local component, select it and click **Start**.

You must restart the HTTP node's OC4J process whenever you restart the Oracle Files domain. See ["Managing HTTP Nodes"](#) on page 5-5 for more information.

- To stop the entire domain, click **Stop Domain**. This action stops everything, including local and remote components. To stop a single local component, select it and click **Stop**.
- To refresh the domain with the latest changes, click **Refresh Components**. This action will update the domain with the latest node changes, including nodes added, nodes removed, and nodes marked active or inactive.

If the selection button for a particular component is greyed out, that component is not located on the local host. Connect to the Oracle Enterprise Manager Web site on the remote host to start or stop these components.

You can also migrate the domain controller from another host to the local host. See ["Migrating the Domain Controller"](#) in the following section for more information.

## Migrating the Domain Controller

The domain controller is one of the most critical components of the Oracle Files domain. The domain controller establishes control over the nodes that make up the domain, starts and stops the domain, and performs a variety of other tasks. For this reason, it is important to ensure that the domain controller is running.

An administrator's ability to manage the domain decreases significantly when the domain controller goes down, even though some portions of the domain may still be usable. To avoid compromising the availability of the system, you can migrate the domain controller to another middle-tier host. This option allows you to re-enable the domain controller even when the middle-tier instance that hosted the domain controller fails.

---

**Note:** You can only migrate the domain controller when it is not running.

---

## Migrating the Domain Controller to a New Middle-Tier Host

New middle-tier hosts are set up through the Oracle Files Configuration Assistant. During the process of configuration, you can indicate whether the domain controller is to be run on the new middle-tier host.

The domain controller will be migrated to the new domain instance as part of the configuration process. See the Oracle Files chapter of the *Oracle Collaboration Suite Installation and Configuration Guide* for instructions on how to set up a new middle tier using the Oracle Files Configuration Assistant.

## Migrating the Domain Controller to an Existing Middle-Tier Host

You can migrate the domain controller to an existing middle-tier instance using the Oracle Enterprise Manager Web site.

The following steps assume that the domain controller is currently on Host 1, and you wish to migrate it to Host 2.

1. Access the Oracle Enterprise Manager Web site for Host 2 (in other words, the host where you want the domain controller to be migrated).
2. Navigate to the Oracle Files Home page.

**Figure 5–3 Oracle Files Home Page With Configure Domain Controller Button**

ifs://samman-sun:1521:ora92db:FILESDROP

Refreshed at Tuesday, March 4, 2003 1:23:14 PM PST

**General**

Domain Name: ifs://samman-sun:1521:ora92db:FILESDROP  
Domain Type: Unavailable

**Components**

Start Local Components Stop Domain Refresh Components Configure Domain Controller

An Internet File System domain contains a Domain Controller and a set of Nodes.

Select	Name	Type	Status	Host	Is Local?
<input type="radio"/>	Domain Controller	Domain Controller	❌	hkolpuru-sun.us.oracle.com	No
<input type="radio"/>	hkolpuru-sun.us.oracle.com HTTP Node	HTTP Node	?	hkolpuru-sun.us.oracle.com	No
<input type="radio"/>	hkolpuru-sun.us.oracle.com Node	Node	?	hkolpuru-sun.us.oracle.com	No

3. Click **Configure Domain Controller**.
4. On the Confirmation page, click **OK**. The domain controller is migrated to the local host (Host 2).

## Managing the Node Processes

There are two types of nodes: regular nodes and HTTP nodes. Although the domain can contain nodes on multiple middle-tier hosts, you can only start and stop nodes that are on your local host.

### Managing Regular Nodes

The following sections explain how to start and stop regular nodes using the Oracle Enterprise Manager Web site.

#### Starting Regular Nodes

1. On the Oracle Files Home page, select the regular node that you want to start from the Components table.
2. Click **Start**.

The Node status column displays a checkmark icon, indicating that the node is up.

#### Stopping Regular Nodes

1. On the Oracle Files Home page, select the node to be stopped.
2. Click **Stop**.
3. On the Warning page, click **Yes** to stop the node.

The Node status column displays a down arrow icon, indicating that the node is down.

To permanently delete a node from the domain, you must either delete the node configuration object, or mark the node configuration inactive by deselecting the **Active** checkbox from the Edit Node Configuration page. See "[Changing a Node Configuration](#)" on page 4-3 for information about making a node configuration inactive. See "[Deleting a Node Configuration](#)" on page 4-7 for information about deleting node configuration objects.

### Managing HTTP Nodes

HTTP nodes run in OC4J instances. The default OC4J instance name for Oracle Files is `OC4J_iFS_files`.

The following sections explain how to start and stop HTTP nodes using the Oracle Enterprise Manager Web site. You can also use `opmnctl` to start and stop HTTP nodes; see "[Managing OC4J Processes](#)" on page 5-9 for more information.

#### Starting HTTP Nodes

1. Go to the Oracle*9i*AS Home page.
2. Select the OC4J instance for the HTTP node from the System Components table.
3. Click **Start** or **Restart**.

---

---

**Note:** You must restart the OC4J instance whenever you restart the Oracle Files domain.

---

---

#### Stopping HTTP Nodes

To stop HTTP nodes using the Oracle Enterprise Manager Web site:

1. Go to the Oracle*9i*AS Home page.
2. Select the OC4J instance for the HTTP node from the System Components table.
3. Click **Stop**.
4. On the Warning page, click **Yes** to stop the OC4J instance.

---

**Tip:** Use the following `dcmctl` command to check the status of the HTTP node:

```
dcmctl getState -co OC4J_iFS_files -v
```

The `dcmctl` command-line tool is located in `$ORACLE_HOME/dcm/bin`.

---

### Permanently Deleting an HTTP Node

You cannot delete the OC4J instance for an HTTP node (`OC4J_iFS_files`), because these OC4J instances are created as protected instances. They cannot be deleted either through the Oracle Enterprise Manager Web site or through `dcmctl`; they can only be disabled.

Once the OC4J instance is disabled, Oracle Enterprise Manager or `opmnctl` will no longer attempt to start it.

To permanently remove an HTTP node, you must do the following:

1. Stop the OC4J instance for the HTTP node you want to remove.
2. Disable the OC4J instance:
  - a. From the Oracle*9i*AS Home page, click **Enable/Disable Components**.
  - b. On the Enable/Disable Components page, select the OC4J instance you want to disable and move it to the **Disabled Components** list.
  - c. Click **OK**.
3. Delete the node configuration object, or mark the node configuration inactive by deselecting the **Active** checkbox from the Edit Node Configuration page.

See ["Deleting a Node Configuration"](#) on page 4-7 for information about deleting node configuration objects. See ["Changing a Node Configuration"](#) on page 4-3 for information about making a node configuration inactive.

## Starting, Stopping, Suspending, and Resuming Servers

A *node configuration* defines the behavior of a particular node. Which servers and agents start up with the node are determined by the node configuration selected. These servers and agents are started automatically when you start the domain, unless you specify otherwise. You can also manually start servers from the Node page.

---

**Note:** *Server* is a generic term that applies to both protocol servers and agents.

---

1. On the Oracle Files Home page, click the name of the Oracle Files node you want to view. The Node page appears, showing the service and servers that comprise the node (see [Figure 5-4](#)).

2. Examine the Status column for the servers to see which servers are running or are stopped.

You can select a server and click one of the following buttons:

- Start
- Restart
- Suspend
- Resume
- Stop
- Unload

If you click a server name in order to directly edit the server properties, any changes you make remain active for this session only. To permanently change server properties, see ["Changing a Server Configuration"](#) on page 4-15. To change which servers start up automatically, see ["Changing a Node Configuration"](#) on page 4-3.

**Figure 5-4 Services and Servers Sections of Node Page**

**Services**

Start Service

Dispose

Select	Name	Accepting New Session?	Auto Disposed?	Max Concurrent Sessions	Max Concurrent Sessions Per User
<input type="radio"/>	ifsDefaultService	Yes	No	Unlimited	Unlimited

**Servers**

Load Server

Start Restart Suspend Resume Stop Unload

Select	Name	Type	Status	Service	Priority
<input type="radio"/>	FilesSubscriberExpirationAgent	AGENT	Running	ifsDefaultService	5
<input type="radio"/>	FilesSubscriberUsageAgent	AGENT	Running	ifsDefaultService	5
<input type="radio"/>	AfpServer	AFP	Running	ifsDefaultService	5
<input type="radio"/>	SmbServer	SMB	Running	ifsDefaultService	5
<input type="radio"/>	ServiceWarmupAgent	AGENT	Stopped	ifsDefaultService	5
<input type="radio"/>	FilesWorkflowLockCleanupAgent	AGENT	Running	ifsDefaultService	5
<input type="radio"/>	FilesReviewProcessExpirationAgent	AGENT	Running	ifsDefaultService	5
<input type="radio"/>	LockAgent	AGENT	Running	ifsDefaultService	5
<input type="radio"/>	PrintAgent	AGENT	Running	ifsDefaultService	5
<input type="radio"/>	AccessControlListIndexAgent	AGENT	Running	ifsDefaultService	5
<input type="radio"/>	GarbageCollectionAgent	AGENT	Running	ifsDefaultService	5

## Loading and Unloading Servers

In addition to starting and stopping servers, you can load and unload servers. Stopping/Starting (Restart) and Unloading/Loading are very different functions:

- Restart stops and then starts the server. You can only restart servers that are started.
- Unloading/Loading 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).

You must Unload/Load the server for changes to configuration properties to take effect. Restarting the server will not pick up the changes. See ["Reloading Servers"](#) on page 6-16 for more information.

## Managing the Oracle Files Domain from the Command Line

As an alternative to using the Oracle Enterprise Manager Web site to start the domain and nodes, you can use the `ifsctl` command-line tool. The tool is located in:

```
$ORACLE_HOME/ifs/files/bin/
```

The general syntax is:

```
ifsctl command [switch ...] [argument ...]
```

For example:

```
ifsctl stop -v ifs://testcomputer.us.oracle.com:1521:filesservice:filesschema
```

Some commands require a schema password. In those instances, `ifsctl` prompts for the password, either on the terminal (UNIX) or using a dialog box (Windows).

The `ifsctl` commands are summarized in [Table 5–1](#). For more details on the commands, type `ifsctl`.

**Table 5–1** *ifsctl* Commands

Command	Use
<code>ifsctl start [-v]<sup>1</sup> [-n]<sup>2</sup> [domain]<sup>3</sup></code>	Launches any local Oracle Files nodes for the specified domain. ("Local nodes" are those configured to run on the computer where <code>ifsctl</code> is invoked.) If the domain controller for the specified domain runs locally, it is also launched. If domain is omitted, all local Oracle Files nodes and domain controllers for all domains for which the computer is registered are launched. The command also starts the domain controller if it has been launched (either locally or remotely) but is not yet started.  If you include <code>-n</code> , the Oracle Files nodes and domain controllers are still launched, but the domain controller is not started (since starting an Oracle CM SDK domain requires a schema password).
<code>ifsctl stop [-v] [domain]</code>	Stops the specified domain. The domain controller and all nodes, whether local or remote, are stopped. If only one domain is registered for the computer, the domain may be omitted.
<code>ifsctl stoplocalnodes [-v] [domain]</code>	Stops the local nodes for the specified domain. Nodes running on other computers are not affected. The domain controller is not stopped. If only one domain is registered for the computer, the domain may be omitted.

**Table 5–1 (Cont.) ifscctl Commands**

Command	Use
<code>ifscctl status [-v] [-n] [domain]</code>	Displays the status of the specified domain. If the domain is omitted, displays the status for all domains for which the computer is registered.
<code>ifscctl validateconfiguration [-v] [-p]<sup>4</sup> [domain]</code>	Synchronizes the Oracle Files registry file (on the local computer) with the domain registry (in the Oracle Files schema). This is normally done automatically; however, if the local computer's file system was restored from a backup (for example, after a disk failure), explicit synchronization might be required.

<sup>1</sup> All commands support a -v, "verbose" switch. This causes ifscctl to generate a log file with additional diagnostic information, located at \$ORACLE\_HOME/ifs/files/log/ifscctl.log.

<sup>2</sup> Including -n requests non-interactive operation; ifscctl does not prompt for the schema password.

<sup>3</sup> Specify [domain] in the format `ifs://db_host:port:db_service:files_schema`. You only need to specify [domain] when you have multiple Oracle Files domains on the same host.

<sup>4</sup> -p means "prune." If the registry file contains a domain that no longer exists (namely, if Oracle Files cannot connect to the database schema for that domain), the computer is deregistered from that domain.

## Managing OC4J Processes

Oracle Files HTTP nodes run in OC4J processes. Because OC4J processes are not owned by Oracle Files (and might also be running non-Oracle Files servlets), ifscctl does not launch or stop OC4J processes. Use the Oracle Enterprise Manager Web site for this purpose, or you can run the following commands:

```
opmnctl startproc gid=OC4J_iFS_files
opmnctl restartproc gid=OC4J_iFS_files
opmnctl stopproc gid=OC4J_iFS_files
opmnctl status
```

You can run the OPMN command line from:

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

See ["Oracle Process Management and Notification"](#) in the following section for more information.

Assuming the domain controller is running, when an OC4J process is launched, any Oracle Files HTTP nodes configured to run in that OC4J instance are automatically started. When an OC4J process is stopped, the HTTP nodes are stopped. Although ifscctl doesn't start and stop HTTP nodes, it does display their status.

## Oracle Process Management and Notification

Oracle Process Management and Notification (OPMN) manages all the components within an application server instance, including Oracle HTTP Server, OC4J processes, and Oracle9iAS Web Cache. It channels all events from different components to all components interested in receiving them. OPMN consists of two components:

- Oracle Process Manager (PM) is the centralized process management mechanism in Oracle9i Application Server and manages all Oracle9iAS component processes. It starts, stops, restarts, and detects the termination of these processes. When these processes are configured to start up, the characteristics of each set are specified in a configuration file:

`$ORACLE_HOME/opmn/conf/opmn.xml`

The PM starts and then waits for a command to start specific processes or all processes. At shutdown, the PM receives a request to stop one or more processes, or all processes and itself.

- Oracle Notification System (ONS) is the transport mechanism for failure, recovery, startup, and other related notifications between components in Oracle9i Application Server.

---

**Note:** OPMN cannot manage the Oracle Files domain controller process or the Oracle Files regular node processes.

---

To start Oracle HTTP Server, OC4J, and other processes, you can:

- Use the Oracle Enterprise Manager Web site. On the Oracle9iAS Home page, select the relevant processes and click **Start**.

Or:

- Use the OPMN command line in:

`$ORACLE_HOME/opmn/bin/opmnctl`

For more information on `opmnctl` syntax and usage, see the *Oracle9i Application Server Administrator's Guide*.



---

## Changing Configuration Settings

There are four types of configuration settings in Oracle Files: domain, node configuration, service configuration, and server configuration properties. This chapter tells you how to use the Oracle Enterprise Manager Web site to manage these settings. Topics include:

- [About Configuration Settings](#)
- [Domain Properties](#)
- [Node Configuration](#)
- [Service Configuration](#)
- [Server Configuration](#)
- [Oracle Files Configuration Options](#)
- [Running Oracle Files on Port 80](#)

### About Configuration Settings

The default domain configuration is based initially on the settings you selected during installation and configuration. When the domain is started, it uses the settings contained in the repository to determine which nodes it should control (what nodes comprise the domain). The node configuration defines the runtime behavior of the nodes. The service configuration specifies the size of service each node supports (small, medium, or large). The server configuration determines the protocol servers and agents (AFP, FTP, NFS, and so on) that each service offers for use of the system.

Use the Oracle Enterprise Manager Web site to access a specific configuration object and modify its properties.

### Domain Properties

Domain properties are settings that apply to the entire domain, or to the domain controller. You can view all the domain properties using the Oracle Enterprise Manager Web site. Only underlined properties may be changed. You can add new domain properties, but you cannot remove domain properties.

### Changing Domain Properties

To make changes to the domain configuration properties:

1. From the Oracle9iAS Instance Home page, click the Oracle Files link. The Oracle Files Home page appears.

2. In the Configuration section, select **Domain Properties**.
3. On the Domain Properties page, click the name of the property you want to change. You may need to move to the second or subsequent page to find some properties. Only those properties that are underlined may be changed.
4. Make the changes to the property and click **OK**.
5. For `IFS.DOMAIN.DOMAINCONTROLLER.*` properties, you must restart the domain controller for changes to take effect. For all other domain properties, you must restart the domain for changes to take effect.

You can change these properties:

- `IFS.DOMAIN.APPLICATION.FILES.WorkflowSchemaName`. The name of the Workflow Schema, if Oracle Files was configured to run with Oracle Workflow during installation. Update this value as needed.
- `IFS.DOMAIN.CREDENTIALMANAGER.AnonymousUserName`. The name of the guest user account for this domain. Required. Defaults to: `guest`.
- `IFS.DOMAIN.DOMAINCONTROLLER.CheckNodesPeriod`. The interval between successive checks of the domain's nodes, in seconds. Optional. Defaults to 15 seconds.
- `IFS.DOMAIN.DOMAINCONTROLLER.LogFilename`. The absolute path to the domain controller's log file. Optional. If not specified, logs are generated to the console (`stdout`).
- `IFS.DOMAIN.DOMAINCONTROLLER.LogLevel`. The verbosity of the domain controller log. Optional. Must be one of the following values:
  - 0 = disabled (no logging)
  - 2 = low (error conditions only)
  - 4 = medium (normal operation)
  - 6 = high (debug information)Defaults to 4.
- `IFS.DOMAIN.DOMAINCONTROLLER.OverwriteLog`. Whether any existing log file is overwritten each time the domain controller starts. Optional. Defaults to false and appends the log to any existing log file.
- `IFS.DOMAIN.DOMAINCONTROLLER.RemoterLogLevel`. The verbosity of the inter-process communication log. Optional. Must be one of the following values:
  - 0 = disabled (no logging)
  - 2 = low (error conditions only)
  - 4 = medium (normal operation)
  - 6 = high (debug information)Defaults to 2.
- `IFS.DOMAIN.DOMAINREGISTRY.PasswordRequired`. Whether the domain registry schema requires a password. Defaults to false.
- `IFS.DOMAIN.LIBRARYOBJECT.SERVICECONFIGURATION.DefaultServiceConfiguration`. Defaults to `SmallServiceConfiguration`.

- `IFS.DOMAIN.PROTOCOL.NFS.UidToUserMap`. See ["Mapping UNIX UIDs to Oracle Files User Accounts"](#) on page 2-9 for more information. You may have to move to the second or subsequent page to see this information.

## Node Configuration

The runtime behavior of any node is specified in its *node configuration* object. Each node has its own node configuration. In the Oracle Enterprise Manager Web site, you can dynamically change the node configuration, change to a different configuration, alter a node configuration permanently, create a new node configuration, or delete a node configuration that is no longer needed. Depending on whether you select the HTTP node or a regular node, different properties are changeable.

## Changing a Node Configuration

1. From the Configuration section on the Oracle Files Home page, click **Node Configurations**.
2. On the Node Configurations page, click the name of the node configuration you want to change, either the HTTP node or the regular node. The Edit page appears.
3. Change the General node configuration properties as desired. You can make the following modifications:

**Table 6–1 Node Configuration Properties**

Property	Regular Node	HTTP Node
<b>Description</b> of the node configuration.	Yes	Yes
<b>Access Control</b> level associated with the node configuration.	Yes	Yes
<b>Active</b> status. Deselect to make inactive.  Making a node inactive is a good alternative to deleting the node configuration; it allows you to keep the configuration information, and you can easily activate the node later.  After you make a node inactive, go to the Oracle Files Home page and click <b>Refresh Components</b> to refresh the domain information.	Yes	Yes
<b>Guarded.</b> Whether the node's guardian runs as a separate process. Defaults to true.	Yes	No
<b>Java Command.</b> For guarded nodes, the command issued by the node guardian to create a node manager process. Defaults to java.	Yes  Edit the value to specify command-line arguments for the Java VM, such as <code>java -Xmx512M</code> to increase the maximum size of the Java VM's heap.  To log all garbage collection activity, add <code>-verbosegc</code> as an argument.	Yes  The Java Command and arguments for HTTP nodes are defined in <code>\$ORACLE_HOME/opmn/conf/opmn.xml</code> , in the <code>java-option</code> property for the OC4J instance that corresponds to the HTTP node.

**Table 6–1 (Cont.) Node Configuration Properties**

Property	Regular Node	HTTP Node
<b>Log File.</b> Specifies the location and file name of the node log. If not specified, logs are generated to the console.	Yes	No
<b>Log Level.</b> Verbosity level of the node log. 0 = Disabled (no logging) 2 = Low (error conditions only) 4 = Medium (normal operation; default) 6 = High (debug information) NTFS will not write into the node log unless the Log Level is set to 6 (High).	Yes	Yes
<b>Remoter Log Level.</b> Verbosity level of the inter-process communication log. 0 = Disabled (no logging) 2 = Low (error conditions only; default) 4 = Medium (normal operation) 6 = High (debug information)	Yes	Yes
<b>Log Rotation Interval.</b> The interval in hours that the log file is archived and rotated. Although you can specify 0 to disable log rotation, you should specify an interval in order to prevent the log file from growing too large.	Yes	No
<b>Overwrite Log.</b> Whether any existing log file is overwritten each time the node starts. Defaults to false and appends the log to the existing log file.	Yes	No

4. You can add, edit, or remove services for this node.
  - To add a service, click **Add** under the Services heading, specify information for the service, and click **OK**.
  - 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.
5. You can add, edit, and remove servers for this node.
  - To add a server, click **Add** under the Servers heading, specify information for the server, and click **OK**.
  - 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 up when the node is started, select **Initially Started** on the Edit Server page.
  - To remove a server, select it and click **Remove**.
6. Click **OK** on the Edit Node page to save the changes. You must restart the node in order for your changes to take effect.

## Creating a Regular Node Configuration

1. From the Configuration section on the Oracle Files Home Page, click **Node Configurations**.
2. On the Node Configurations page, decide whether to create a new regular node from scratch or to base it on the properties of an existing node.
  - To create the node from scratch, click **Create**.
  - To base the node on an existing node, select that node's checkbox and click **Create Like**.

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

**Figure 6–1 New Node Configuration Page**

**New Node Configuration** Cancel OK

Click "OK" to create the object, or "Cancel" to cancel this operation.  
\* Indicates a required field

**General**

\* Name

Type ☐ HTTP Node ☒ Non-HTTP Node  
Only HTTP nodes run in OC4J instances

Description

Access Control  ☐ Active ☐ Guarded  
Applicable to non-HTTP nodes only

Java Command

Log File

Log Level  Applicable to non-HTTP nodes only

Remoter Log Level

Log Rotation Interval (hours)  Applicable to non-HTTP nodes only  
Set to 0 to disable log rotation

☐ Overwrite Log

**Services** Return to Top Add

Select Name	Configuration	Active
No items found		

**Servers** Return to Top Add

You need to add an active Service before you can add any Server.

Select Name	Configuration	Active	Service	Initial Priority	Initially Started
No items found					

3. Enter or change the node information:
  - Name of the node.
  - Type of the node; select **Non-HTTP Node**.  
See [Table 6–1](#) on page 6-3 for more information about general node configuration parameters.
4. Click **Add** 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 service's configuration properties.

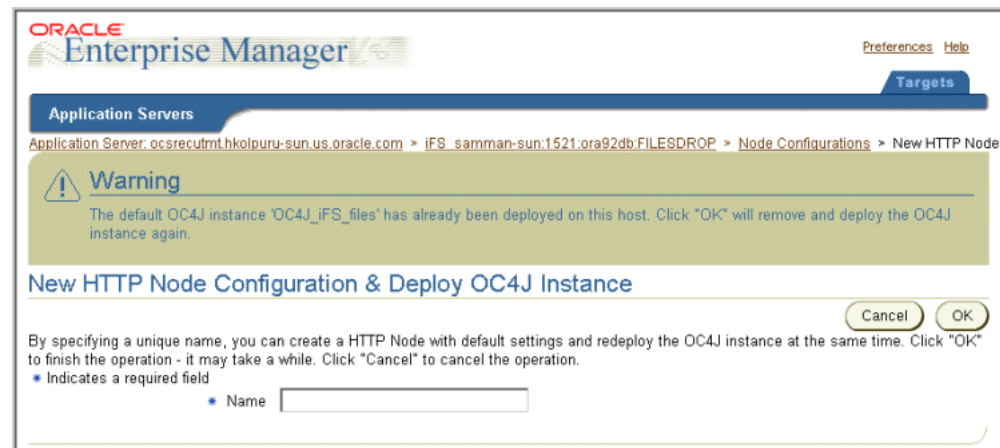
- **Active:** Whether the service is currently active.  
Inactive services are not automatically started by the node. You must have at least one active service in order to add servers to this node configuration.  
When you are finished specifying parameters on the Add Service page, click **OK**.
- 5. 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.
- 6. Click **Add** in the Servers area to choose default servers for the node.  
On the Add Server page, specify:
  - **Name:** Server name.
  - **Configuration:** Which server configuration object provides the server's configuration parameters. For example, select `FtpServerConfiguration` if you want to run an FTP server on this node.
  - **Service:** Name of the service against which the server should 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.When you are finished specifying parameters on the Add Server page, click **OK**.
- 7. 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 up when the node is started, select **Initially Started** on the Edit Server page.
  - To remove a server, select it and click **Remove**.
- 8. Click **OK** on the New Node Configuration page.

## Creating an HTTP Node Configuration

You cannot follow exactly the same procedure as in "[Creating a Regular Node Configuration](#)" to create an HTTP node configuration. You need to create and deploy a corresponding OC4J instance for the HTTP node.

To create an HTTP node and also deploy its OC4J instance:

1. From the Configuration section on the Oracle Files Home page, click **Node Configurations**.
2. On the Node Configurations page, click **Create and Deploy HTTP Node**. The New HTTP Node Configuration & Deploy OC4J Instance page appears:

**Figure 6–2 New HTTP Node Configuration & Deploy OC4J Instance Page**

3. Enter a name for the HTTP node.
4. Click **OK**.
5. Return to the Oracle Files Home Page and click **Refresh Components**.
6. Navigate to the Oracle9iAS Home Page, select the OC4J instance for the HTTP node (**OC4J\_iFS\_files**), and click **Start** or **Restart**.

This operation will deploy the default OC4J instance (OC4J\_iFS\_files). If you already have an HTTP node on the host, this operation removes the currently deployed OC4J instance and redeploys the OC4J\_iFS\_files instance again. Any custom changes that were made to the existing OC4J instance will be lost. This results in the original HTTP node not functioning anymore. You should delete the node configuration for the original HTTP node.

## Deleting a Node Configuration

As an alternative to deleting a node configuration, consider making a node inactive instead. This option allows you to keep the configuration information, and you can easily activate the node later. See ["Changing a Node Configuration"](#) on page 6-3 for more information.

To delete a node configuration:

1. On the Oracle Files Home Page, in the Configuration section, click **Node Configurations**.
2. On the Node Configurations page, select the node configuration you want to delete.
3. Click **Delete**.
4. On the Warning page, click **Yes**. The node configuration is deleted.

---

**Note:** To permanently delete an HTTP node from the domain, you must delete the node configuration object and disable its OC4J instance. See ["Permanently Deleting an HTTP Node"](#) on page 5-6 for more information.

---

## Service Configuration

A *service configuration* holds the default values used when a service is started for an Oracle Files node. Each service configuration specifies values for properties such as the database instance and schema name of the Oracle Files repository, credential manager settings, the sizes of the cache and database connection pools, the maximum number of sessions, and the service's default language and character set. (See [Appendix B, "Service Configuration Reference"](#) for a complete list of service configuration parameters.) Service configurations are uniquely named across the domain.

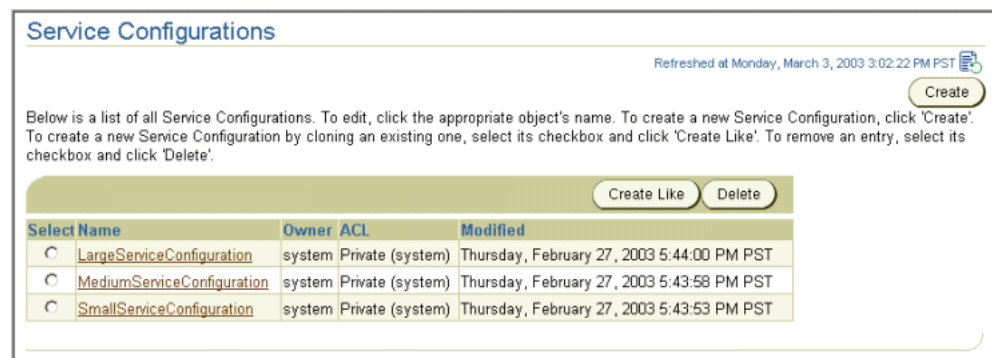
Whenever a new Oracle Files schema is created, three service configuration objects are generated:

- SmallServiceConfiguration
- MediumServiceConfiguration,
- LargeServiceConfiguration

These objects are named to reflect the sizes of their data caches. For information about which service configuration object to use, see the *Oracle Files Planning Guide*.

Use the Oracle Enterprise Manager Web site to create or edit service configuration objects (see [Figure 6-3](#)). 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 particular service while it is running.

**Figure 6-3 Service Configurations Page**



Like the node configuration, you can dynamically change the service configuration properties, change to a different configuration, alter a service configuration permanently, or create a new service configuration.

## Changing a Service Configuration

1. From the Configuration section on the Oracle Files Home Page, click **Service Configurations**.
2. On the Service Configurations page, click the name of the service configuration you want to change. The Edit page appears.
3. You can change general information about the service as well as the properties of the service.

**General information.** Change the description of the service or the access control assigned to the service.



**Properties.** Click the name of the property you want to change to display the Edit page. Change the values shown as desired.

4. Click **OK** to save the changes. You must restart all nodes that use this service configuration in order for your changes to take effect.

## Creating a Service Configuration

1. From the Configuration section on the Oracle Files Home Page, click **Service Configurations**.
2. On the Service Configurations page, decide whether to create a new service from scratch or to base it on the properties of an existing node.
  - To base the service on an existing service, select that service's checkbox and click **Create Like** (recommended).
  - To create the service from scratch, click **Create**.

In both cases, the New Service Configuration page appears. If you selected **Create Like**, the properties have been filled in with those of the selected existing service.

**Figure 6–4 New Service Configuration Page**

**New Service Configuration**

Cancel OK

Click "OK" to create the object, or "Cancel" to cancel this operation.  
 \* Indicates a required field

**General**

\* Name

Description

Access Control

**Properties**

Add Remove

Previous 1-25 of 81 Next 25

Select	Name	Type	Value
<input type="radio"/>	IFS_SERVICE_ACLCACHE_EmergencyTrigger	INTEGER	600
<input type="radio"/>	IFS_SERVICE_ACLCACHE_NormalTrigger	INTEGER	500
<input type="radio"/>	IFS_SERVICE_ACLCACHE_PurgeTarget	INTEGER	400
<input type="radio"/>	IFS_SERVICE_ACLCACHE_Size	INTEGER	750
<input type="radio"/>	IFS_SERVICE_ACLCACHE_UrgentTrigger	INTEGER	550
<input type="radio"/>	IFS_SERVICE_CONNECTIONPOOL_READONLY_MaximumSize	INTEGER	20
<input type="radio"/>	IFS_SERVICE_CONNECTIONPOOL_READONLY_MaximumSizeTimeout	INTEGER	10000
<input type="radio"/>	IFS_SERVICE_CONNECTIONPOOL_READONLY_MinimumSize	INTEGER	2

3. Enter a service name.
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 new service's properties.
7. Click **OK**.

## Runtime Service Configuration

You can make a number of changes to the service during runtime:

- You can specify whether the number of concurrent sessions should be unlimited, or you can limit the sessions to a maximum number.
- You can specify whether the number of concurrent sessions per user should be unlimited, or you can limit the sessions to a maximum number.
- You can enable or disable the acceptance of new sessions.
- You can specify whether the service should shut down automatically when the last session is disconnected.

You can also dynamically configure the Committed Data Cache, Read-only Connection Pool, and the Writeable Connection Pool while the service runs.

---

**Note:** Any dynamic changes will be lost when the node is restarted. To permanently change service configuration settings, including Committed Data Cache, Read-only Connection Pool, and Writeable Connection Pool settings, you must change the appropriate properties in the service configuration object (see ["Changing a Service Configuration"](#) on page 6-8 for more information).

---

### About the Committed Data Cache

The Committed Data Cache provides caching of the attribute values of frequently used objects without a database request, greatly improving performance and scalability. Data that has not been least recently used is periodically purged from the cache.

You can dynamically change the properties of the Committed Data Cache from the Committed Data Cache Administration page. See ["Monitoring Service Performance"](#) on page 7-3 for information about viewing or resetting the statistics.

### About the Read-Only Connection Pool

The Read-Only Connection Pool dynamically displays the total and allocated connections, the immediate, deferred, and failed allocations, and the average allocation time. The Read-Only Connection Pool is 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.

You can dynamically change the properties of the Read-Only Connection Pool from the Connection Pool Administration page. See ["Monitoring Service Performance"](#) on page 7-3 for information about viewing or resetting the statistics.

### About the Writable Connection Pool

The Writable 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 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.

You can dynamically change the properties of the Writable Connection Pool from the Connection Pool Administration page. See "[Monitoring Service Performance](#)" on page 7-3 for information about viewing or resetting the statistics.

### Dynamically Changing Data Cache and Connection Pool Configuration

Use the Oracle Enterprise Manager Web site to dynamically change settings for the Committed Data Cache, as well as for the Read-Only and Writable Connection Pools.

1. On the Oracle Files Home page, click the node whose service you want to configure.
2. On the Node page, click the service (for example, `IfsDefaultService`).
3. For **Concurrent Sessions**, choose **Unlimited** or **Limited**. If you choose **Limited**, specify the maximum number of sessions.
4. For **Concurrent Sessions Per User**, choose **Unlimited** or **Limited**. If you choose **Limited**, specify the maximum number of sessions.
5. Select **Accepting New Sessions** if you want this service to accept new sessions.
6. Select **Disposed on Last Disconnected Session** if you want this service to shut down automatically when the last session is disconnected.
7. To configure the committed data cache, click **Committed Data Cache Configuration** in the Configuration section. Continue with Step 8.

Or:

To configure the read-only or writeable connection pool, click **Connection Pool Configuration** in the Configuration section. Continue with Step 9.

8. Change the parameters on the Committed Data Cache Configuration page as desired.

**Figure 6–5 Committed Data Cache Configuration Page**

**Table 6–2 Committed Data Cache Configuration Properties**

Property	Description
Cache Capacity	The absolute maximum size of the service's data cache, in LibraryObjects. The service data cache holds the attribute values of recently used LibraryObjects. Defaults to 7500.
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. Defaults to 5000.

**Table 6–2 (Cont.) Committed Data Cache Configuration Properties**

Property	Description
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. Must be greater than <code>IFS.SERVICE.DATACACHE.NormalTrigger</code> . Defaults to 5500.
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. Must be greater than <code>IFS.SERVICE.DATACACHE.UrgentTrigger</code> but less than <code>IFS.SERVICE.DATACACHE.Size</code> . Defaults to 6000.
Purge Target	The target cache size, in LibraryObjects, upon completion of a purge cycle. Must be less than <code>IFS.SERVICE.DATACACHE.NormalTrigger</code> . Defaults to 4000.

9. Change the parameters on the Connection Pool Configuration page as desired.

**Figure 6–6 Connection Pool Configuration Page**

The screenshot shows the 'Connection Pool Configuration' page. At the top right, it says 'Refreshed at Thursday, March 6, 2003 10:13:21 AM PST' with a refresh icon. Below this are three buttons: 'Cancel', 'Revert', and 'Apply'. A note states: 'Click "Apply" to commit the changes and remain on this page, "Revert" to discard the changes and restore to original values, or "Cancel" to cancel this operation.' Below the note is a legend: '\* Indicates a required field'.

The page is divided into two sections: 'Readonly Connection Pool' and 'Writeable Connection Pool'.

**Readonly Connection Pool:**

- \* Minimum Number of Connections: 2
- \* Target Maximum Number of Connections: 10
- \* Absolute Maximum Number of Connections: 20
- \* Target Size Timeout (msec): 1,000
- \* Maximum Size Timeout (msec): 10,000
- 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
- \* Target Size Timeout (msec): 1,000
- \* Maximum Size Timeout (msec): 10,000
- Default Number of Rows Prefetched: 0

**Table 6–3 Read-Only Connection Pool Configuration Properties**

Property	Description
Minimum Number of Connections	The initial number of database connections in the read-only connection pool. Defaults to 2.  If you change this property, make sure the value you specify is greater than the current connection pool size. You can view the current connection pool size from the Connection Pool Statistics page; see <a href="#">"Monitoring Node Performance"</a> on page 7-3 for more information.
Target Maximum Number of Connections	The target maximum number of database connections in the read-only connection pool. Must be greater than or equal to <code>IFS.SERVICE.CONNECTIONPOOL.READONLY.MinimumSize</code> . Defaults to 10.
Absolute Maximum Number of Connections	The absolute maximum number of database connections in the read-only connection pool. Must be greater than or equal to <code>IFS.SERVICE.CONNECTIONPOOL.READONLY.TargetSize</code> . Defaults to 20.

**Table 6–3 (Cont.) Read-Only Connection Pool Configuration Properties**

Property	Description
Target Size Timeout	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. Defaults to 1000.
Maximum Size Timeout	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 be thrown. Defaults to 10,000.

**Table 6–4 Writable Connection Pool Configuration Properties**

Property	Description
Minimum Number of Connections	The initial number of database connections in the writable connection pool. Defaults to 2.  If you change this property, make sure the value you specify is greater than the current connection pool size. You can view the current connection pool size from the Connection Pool Statistics page; see <a href="#">"Monitoring Node Performance"</a> on page 7-3 for more information.
Target Maximum Number of Connections	The target maximum number of database connections in the writable connection pool. Must be greater than or equal to <code>IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MinimumSize</code> . Defaults to 10.
Absolute Maximum Number of Connections	The absolute maximum number of database connections in the writable connection pool. Must be greater than or equal to <code>IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSize</code> . Defaults to 20.
Target Size Timeout	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 writable 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. Defaults to 1000.
Maximum Size Timeout	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 writable 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 be thrown. Defaults to 10,000.

## Server Configuration

A *server configuration* holds the default values used when a server is started for an Oracle Files node. 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 C, "Server Configuration Properties"](#)). For example, a server configuration for the Oracle Files FTP server specifies the FTP

port number, whether anonymous FTP connections are allowed, and the connection time out 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 Files 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 Oracle Enterprise Manager Web site. Any changes you make will be reflected the next time the node is restarted or when the server is unloaded and then loaded again.

## Abstract vs. Non-abstract Server Configuration

Server configuration objects are created for each protocol server and agent as part of the configuration of Oracle Files. These objects in turn have a number of properties that are used by the respective servers and agents. These properties are assigned certain values by default.

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 any abstract server configuration.
- **Non-abstract:** Can be used to start servers.

When you create a new server configuration, you can choose to inherit the properties from one or more server configurations. These in turn bring into play their own properties and their respective values. You could choose to use the same values as inherited or to use different values.

Inheritance operations are accessed from the New Server Configuration page (Figure 6-7). See "Creating a Server Configuration" on page 6-15 for more information on creating new server configurations.

**Figure 6-7 Inheritance Operations on the New Server Configuration Page**

**Inherited Server Configurations** [Return to Top](#)

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.

**Available Configurations**

- AccessControlListIndexAgentConfiguration
- AfpServerConfiguration
- ContentGarbageCollectionAgentConfiguration
- DanglingObjectAVCleanupAgentConfiguration
- DavServerConfiguration
- EventExchangerAgentConfiguration
- ExpirationAgentConfiguration
- FilesAfpServerConfiguration
- FilesArchiveFileToBFileAgentConfiguration
- FilesBaseServerConfiguration

Description

**Inherited Configurations**

Description

**Properties** [Return to Top](#)

Inherited and locally defined properties are shown for the Server Configuration. If you make any change in the inherited Server Configurations, click "Update Inherited Properties" to revise the inherited properties. Click "Add" or "Edit" or "Remove" to manage locally defined properties.

[Update Inherited Properties](#) [Add](#)

Select Name	Inherited	Type	Value
No items found			

## Change Values of Properties

Create a new property in the inherited server configuration object that is identical in name to the one in the parent, but has values that override those in the parent server configuration object.

## View 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.

## Changing a Server Configuration

Use the Oracle Enterprise Manager Web site to change server configurations.

1. From the Configuration section on the Oracle Files Home Page, click **Server Configurations**.
2. On the Server Configurations page, click the name of the server configuration you want to change.
3. On the Edit page, you can change general information about the server as well as the properties of the server.
  - In the General section, change the description of the server or the access control assigned to the server. Select or de-select **Abstract**.
  - In the Inherited Server Configurations section, select or de-select the existing configurations from which the configuration should inherit properties.
  - In the Properties section, click **Show Inherited Properties** to display the properties of the inherited server configurations.
    - Delete any of the locally-defined properties by selecting the checkbox and clicking **Remove**.
    - You can edit any property that is locally defined (not inherited) by selecting the property and clicking **Edit** to display the Edit page. Change the values and click **OK**.
    - To add a new property, in the Properties section, click **Add**. On the Add Property page, enter the values shown and click **OK**.
4. When the server configuration is complete, click **OK**. Changes take effect when the server is unloaded and then loaded again. Restarting the server will not pick up the changes. See ["Reloading Servers"](#) on page 6-16 for more information.

---

**Note:** See [Appendix C, "Server Configuration Properties"](#) for more information about specific server configuration parameters.

See ["Using Oracle Files with NFS"](#) on page 2-8 for information about configuring the NFS server, including mapping UNIX UIDs to Oracle Files user accounts, setting up a trusted client list, and enabling NIS authentication.

---

## Creating a Server Configuration

Use the Oracle Enterprise Manager Web site to create new server configurations.



1. From the Configuration section on the Oracle Files Home Page, click **Server Configurations**.
2. On the Server Configurations page, decide whether to create a new server configuration from scratch or to base it on the properties of an existing server.
  - To create the server configuration from scratch, click **Create**.
  - To base the server configuration on an existing server configuration, select that server's checkbox and click **Create Like**.

In both cases, the New Server Configuration page appears. If you selected **Create Like**, the properties have been filled in with those of the selected existing server.
3. On the New Server Configuration page, in the General section, enter a name for the new server configuration.
4. Check the **Abstract** box if you want to make this server configuration not instantiable.
5. In the Inherited Server Configurations section, select the existing configurations from which the new configuration should inherit properties. Select configurations from the Available Configurations list and move them to the Selected Configurations list.
6. In the Properties section, click **Update Inherited Properties** to display the properties of the inherited server configurations.
  - Delete any of the locally-defined properties by selecting the checkbox and clicking **Remove**.
  - You can edit any property that is locally defined (not inherited) by selecting the property and clicking **Edit** to display the Edit page. Change the values and click **OK**.
  - To add a new property, in the Properties section, click **Add**.
  - On the Add Property page, enter the name, type, and value and click **OK**.
7. When the server configuration is complete, click **OK**.

## Reloading Servers

If you change a server configuration, you need to unload and then load the server again before the changes take effect. Use the Oracle Enterprise Manager Web site to reload servers.

1. From the Oracle Files Home page, click the name of the node associated with 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 **Stop**. The status should now be "Stopped."
4. Click **Unload**. The server is removed from the Servers list.
5. Click **Load Server**.
6. On the Load Server page, specify the **Server Name**, the **Service Name**, and the **Server Configuration** to use, then click **OK**.
7. Select the server from the Servers list and click **Start**.



## Deleting a Server

Use the Oracle Enterprise Manager Web site to remove a server from a node.

1. From the Oracle Files Home page, click the name of the node associated with the server you want to delete.
2. In the Servers section of the Node page, select the server you want to delete.
3. Click **Stop**. The status changes to "Stopped."
4. Select the server again.
5. Click **Unload**. The server is removed from the Servers list.

## Deleting a Server Configuration

You should not delete a server configuration that is being referenced by a node configuration. If you want to do this, first edit the node configuration to remove the server, then delete the server configuration.

To delete a server configuration:

1. On the Oracle Files Home page, in the Configuration section, select **Server Configurations**.
2. On the Server Configurations page, select the server configuration you want to delete.
3. Click **Delete**.
4. Click **Yes** on the Warning page.

## Oracle Files Configuration Options

The Oracle Enterprise Manager Web site provides additional configuration options critical to the Oracle Collaboration Suite. These components include:

- [Oracle Collaboration Suite Search Configuration](#)
- [Printing Services](#)
- [MIME Type Formats](#)

## Oracle Collaboration Suite Search Configuration

Oracle Collaboration Suite Search, also known as Federated Search, is an application that lets users search configured applications in the Oracle Collaboration Suite. Oracle Collaboration Suite Search can search the following applications:

- Oracle Files
- Oracle Email
- Oracle Voicemail & Fax

You can also configure Oracle Ultra Search to be part of Oracle Collaboration Suite Search. If you enable Oracle Ultra Search, a **Web Sites** checkbox for Oracle Ultra Search will be included on the Oracle Collaboration Suite Search page.

Enabling Oracle Collaboration Suite Search is a post-configuration step dependent on Oracle Email and Oracle Ultra Search configuration. You must configure Oracle Files in order to use Oracle Collaboration Suite Search.

To configure Oracle Collaboration Suite Search:

1. From the Configuration section of the Oracle Files Home page, click **Federated Search Configuration**.
2. On the Federated Search Configuration page, set the appropriate search configuration parameters. See [Table 6–5, "Federated Search Configuration Parameters"](#) for a list of properties.
3. Click **Apply**.

**Figure 6–8 Federated Search Configuration Page**

### Configuring Search Parameters

To enable Oracle Collaboration Suite Search for Oracle Email and Oracle Ultra Search, you must set parameters on the Federated Search Configuration page. If you do not enable Oracle Email or Oracle Ultra Search, the Search page in Oracle Collaboration Suite will only search Oracle Files.

After you set properties on the Federated Search Configuration page, you need to perform several post-configuration steps in Oracle Email and Oracle Ultra Search. See the *Oracle Email Administrator's Guide* and the *Oracle Ultra Search User's Guide* for more information.

Federated Search configuration parameters are listed in [Table 6–5](#). Except for the Ultra Search Schema Password, all properties are stored as Oracle Files domain properties. The Ultra Search Schema Password is stored as an encrypted repository parameter.

**Table 6–5 Federated Search Configuration Parameters**

Property	Description
Mail Configured	Click <b>Yes</b> to enable searching of Oracle Email through Oracle Collaboration Suite Search. If you click <b>Yes</b> , a <b>Mail</b> checkbox will be included on the Oracle Collaboration Suite Search page. Click <b>No</b> if you do not wish to enable searching of Oracle Email, or if you are not using Oracle Email. Clicking <b>Yes</b> will also enable searching of Oracle Voicemail & Fax.
Ultra Search Configured	Click <b>Yes</b> to enable the Oracle Ultra Search application. If you click <b>Yes</b> , a <b>Web Sites</b> checkbox for Oracle Ultra Search will be included on the Oracle Collaboration Suite Search page. Click <b>No</b> if you do not wish to enable the application.
Web Mail Base URL	The base URL to access Oracle WebMail messages. The URL must end with /um/traffic_cop. For example, http://email.example.com:7778/um/traffic_cop
Ultra Search Schema Name	The Oracle Ultra Search schema name.

**Table 6–5 (Cont.) Federated Search Configuration Parameters**

Property	Description
Ultra Search Schema Password	The Oracle Ultra Search schema password.
Confirm Password	Confirmation of the Oracle Ultra Search schema password.
Ultra Search Connection String	A JDBC connection string for the database that contains the Oracle Ultra Search installation. The string must begin with <code>jdbc:oracle:thin:@</code> . For example, <code>jdbc:oracle:thin:@infrastructure_host:1521:iasdb</code>
Ultra Search Mail Page	This property is not used in Oracle Collaboration Suite.

## Printing Services

Oracle Files supports printing to line printer daemon (LPD) printers using the SMB protocol. To integrate with—and allow users to print from—the Oracle Collaboration Suite, a printer must be physically connected to the network using the TCP/IP protocol. This means that a host name or an IP address is required to establish a connection with the network.

Administrators can add, modify, and delete printers:

1. On the Oracle Files Home page, select **Printers** from the Oracle Files Administration section.
2. On the Printers page, you can:
  - Click **New Printer**, and on the Printers page enter the printer configuration information.
  - Select a printer and click **Delete**.
  - Click an existing printer name to modify the printer configuration information.

**Figure 6–9 Adding a Printer**

For information on entering the printer configuration information and completing the process of adding, modifying, or deleting a printer, see the online help for the Oracle Enterprise Manager Web site.

## Notes

- After adding and modifying a printer, both the SMB server and the Print Agent must be reloaded before the new settings are enabled. Click the node from the Oracle Files Home page, and then reload the Print Agent and the SMB server from the Node page.

- After a printer is configured, Windows users must use the Add Printer wizard in the Windows Control Panel to add and enable the printer.

## MIME Type Formats

Oracle Files associates a format (MIME type) with each document. The format of a document specifies the way the document information is encoded. Internet browsers need to know the format of documents to determine how to store and index their contents.

A format contains the following information:

- **MIME type:** Specifies the type of content stored in Oracle Files.
- **Extension type:** Specifies the default extension to use for storing Oracle Files content as a file.
- **Binary setting:** Determines whether the content stored in Oracle Files is of binary type.
- **Index setting:** Determines whether the content of this format should be indexed in Oracle Files.

Indexing a format type is the basis of content searching in Oracle Files. If a format is not indexed, searches will fail. Searches can also fail when formats are indexed incorrectly. For example, an administrator could add a new format called `.fm`, a binary Adobe FrameMaker file. However, the administrator could then erroneously associate a text/plain format to the binary `.fm` file. As a result, searches would not return any content contained in a FrameMaker file because Oracle Files would expect to find text/plain format content in a binary file.

Administrators can create, modify, and delete formats.

1. From the Oracle Files Administration section of the Oracle Files Home page, select **Formats**.
2. On the Formats page, you can:
  - Click **New Format**, and on the New Format page enter the MIME type format information. See [Table 6-6](#) for a list of default formats.
  - Select a format and click **Delete**.
  - Click an existing format name and edit the MIME type format information.

**Figure 6-10 Adding a New MIME Type Format**

Oracle Files - New Format

Click "OK" to create the object, or "Cancel" to cancel this operation.  
\* Indicates a required field

\* Name

\* MimeType

\* Extension

☐ Binary

☐ Indexed

For information on entering the MIME type format configuration information and completing the process of adding, modifying, or deleting MIME type formats, see the online help for the Oracle Enterprise Manager Web site.

**Table 6–6 Default System Formats**

<b>Format Name</b>	<b>Extension</b>	<b>Indexed by Default?</b>	<b>Can Change Index Setting?<sup>1</sup></b>
Apple Quicktime	mov	Yes	No
Apple Quicktime (qt)	qt	Yes	No
Basic audio	au	Yes	No
Bitmap image	bmp	Yes	No
Email Message	eml	Yes	No
Extensible Markup Language	xml	Yes	Yes
GIF	gif	Yes	No
HTML	htm	Yes	Yes
HTML unix	html	Yes	No
JPEG	jpg	Yes	No
JPEG (jpe)	jpe	Yes	No
JPEG (jpeg)	jpeg	Yes	No
JSP	jsp	Yes	Yes
Microsoft AVI	avi	Yes	No
Microsoft PowerPoint	ppt	Yes	Yes
Microsoft Wave Audio	wav	Yes	No
MIDI	mid	No	Yes
MPEG	mpg	Yes	Yes
MPEG (mpe)	mpe	No	Yes
MPEG (mpeg)	mpeg	No	Yes
MPEG Layer 3 Audio	mp3	Yes	No
MS Access	mdb	Yes	Yes
MS Excel	xls	Yes	Yes
MS Word	doc	Yes	Yes
MS Works	msw	Yes	Yes
PCX	pcx	No	Yes
PDF	pdf	Yes	Yes
Postscript	ps	No	Yes
Real Audio (ra)	ra	Yes	No
Real Audio (ram)	ram	Yes	Yes
Real Media (rm)	rm	Yes	No
Real Video	rv	Yes	No
RichText	rtf	Yes	Yes
SGI Video	movie	No	Yes
Standard General Markup Language	sgml	Yes	Yes
Text	txt	Yes	Yes

**Table 6–6 (Cont.) Default System Formats**

Format Name	Extension	Indexed by Default?	Can Change Index Setting? <sup>1</sup>
TIFF	tif	Yes	No
TIFF (tiff)	tiff	Yes	No
Unknown Binary	bin	No	Yes
URL Reference	url	No	Yes
VRML	vrml	No	Yes
Word Perfect	wpd	Yes	Yes
Zip	zip	No	Yes

<sup>1</sup> Some formats must be indexed. For these formats, the index setting cannot be changed.

## Running Oracle Files on Port 80

If you want to change the Oracle Files application port to 80, perform the tasks listed in the following sections:

- [Changing the Port Number in Oracle Workflow](#)
- [Changing the Port Number in Oracle9iAS Web Cache](#)
- [Changing the Port Number in Oracle HTTP Server](#)
- [Registering the New Port with Oracle9iAS Single Sign-On](#)
- [Updating the Base Server Configuration and Restarting OC4J](#)

### Changing the Port Number in Oracle Workflow

If you have integrated Oracle Files with Oracle Workflow, you must change the port number in Oracle Workflow. You must also update the Workflow URL stored in the `FilesBaseServerConfiguration` and then restart the Oracle Files OC4J instance.

To change the port number in Oracle Workflow, follow these steps:

1. Log in to the Oracle Files Web interface as the Workflow Administrator (typically `orcladmin`).
2. Click **Workflow**.
3. From the Workflow page, click **Global Workflow Preferences**.
4. Click **Update**.
5. In the **Workflow Web Agent** field, change the port number to 80.
6. Click **OK** and close the application.

Use the Oracle Enterprise Manager Web site to update the `FilesBaseServerConfiguration` and to restart the Oracle Files OC4J instance. To do this, follow these steps:

1. From the Oracle Files Home page, under the Configuration heading, click **Server Configurations**.
2. On the Server Configurations page, click **FilesBaseServerConfiguration**.
3. On the Edit page, in the Properties section, select **IFS.SERVER.APPLICATION.FILES.WorkflowUrl** and click **Edit**.

4. In the URL displayed in the **Value** field, replace the current port number with 80 and click **OK**.
5. Click **OK** on the Edit Server Configuration page.
6. Navigate to the Oracle9iAS Home page.
7. Select **OC4J\_iFS\_files** and click **Restart**.

## Changing the Port Number in Oracle9iAS Web Cache

If Oracle9iAS Web Cache is enabled, you must change the port number in Oracle9iAS Web Cache. To do this, follow these steps:

1. Start Oracle9iAS Web Cache, if it has not already been started:  

```
$ORACLE_HOME/webcache/bin/webcachectl start
```
2. Using a Web browser, go to `http://mid-tier_host:4000`.
3. Click **Web Cache Manager**. At the prompt, provide the Oracle9iAS Web Cache administrator user name and password. Typically, you can use `administrator/administrator`.
4. In the navigation pane, under the Cache-Specific Configuration heading, click **Listening Ports**.
5. Select the HTTP port (typically 7777) and click **Edit Selected**.
6. Change the **Port Number** to 80 and click **Submit**.
7. Click **Apply Changes**, then click **Restart**.

## Changing the Port Number in Oracle HTTP Server

You must change the port number in Oracle HTTP Server. To do this, edit the `httpd.conf` file and restart OPMN:

1. On the Oracle Files middle tier, navigate to the following directory:  

```
$ORACLE_HOME/Apache/Apache/conf
```
2. Make a backup of the `httpd.conf` file, then open the file for editing.
3. Locate the `PORT` parameter at the bottom of the file, then change the value to 80.
4. Save the file.
5. Restart OPMN using the following command:  

```
$ORACLE_HOME/opmn/bin/opmnctl restartproc
```

## Registering the New Port with Oracle9iAS Single Sign-On

After you change the port number in Oracle HTTP Server, you must register the new port with Oracle9iAS Single Sign-On. To do this, run the single sign-on registration tool, then restart the Oracle HTTP Server.

### Running the Single Sign-On Registration Tool

To run the tool, execute the following command:

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path orclHomePath -host database_host_name -port database_port_number
-sid database_SID -site_name sitename -success_url successurl
```

```
-logout_url logouturl -cancel_url cancelurl -home_url homeurl [-admin_id adminid]
[-admin_info admininfo] -config_mod_osso TRUE -u userid -sso_server_version v1.2
```

Table 6–7 provides information about the parameters passed to the single sign-on registration tool.

**Table 6–7 Single Sign-On Registration Tool Parameters**

Parameter Name	Description
jar	Absolute path to the ossoreg.jar file: \$ORACLE_HOME/sso/lib/ossoreg.jar
oracle_home_path	Absolute path to the Oracle home
host	The infrastructure database host name
port	The infrastructure database port number, typically 1521
sid	The infrastructure database SID, typically iasdb
site_name	Name of the site. Typically, this value is comprised of the Oracle9iAS instance name and the host name ( <i>Oracle9iAS_instance_name.host</i> ). For example: my_instance.myhost.us.oracle.com
success_url	The URL to the routine responsible for establishing the partner application session and session cookies, in the format: http://mid-tier_host.domain:port/osso_login_success The osso_login_success portion of the URL is <i>not</i> a variable. Specify https rather than http if you want the Web client and the Oracle HTTP Server to communicate using SSL.
logout_url	The URL for the logout routine of the application, in the format: http://mid-tier_host.domain:port/osso_logout_success The osso_logout_success portion of the URL is <i>not</i> a variable. Specify https rather than http if you want the Web client and the Oracle HTTP Server to communicate using SSL.
cancel_url	The URL that specifies where the single sign-on server redirects users when they cancel authentication, in the format: http://mid-tier_host.domain:port/
home_url	This URL must be specified in the following format: http://mid-tier_host.domain:port
admin_id	The user name of the mod_osso administrator (optional)
admin_info	Any additional information, such as the e-mail address, about the administrator (optional)
config_mod_osso	If set to TRUE, this parameter indicates that the application being registered is mod_osso. You must include config_mod_osso for the osso.conf file to be generated.
u	The user name that will start the Oracle HTTP Server. In UNIX, this name is usually root. On Windows, it is SYSTEM. The parameter u is mandatory.
sso_server_version	This parameter must be set to v1.2 in Oracle9iAS, Release 2.

## Restarting the Oracle HTTP Server

Use the following command to restart the Oracle HTTP Server:

```
$ORACLE_HOME/opmn/bin/opmnctl restartproc type=ohs
```



## Updating the Base Server Configuration and Restarting OC4J

Use the Oracle Enterprise Manager Web site to update the `FilesBaseServerConfiguration` and to restart the Oracle Files OC4J instance:

1. From the Oracle Files Home page, under the Configuration heading, click **Server Configurations**.
2. On the Server Configurations page, click **FilesBaseServerConfiguration**.
3. On the Edit page, in the Properties section, select **IFS.SERVER.APPLICATION.UIX.ApplicationPort** and click **Edit**.
4. Set the **Value** to 80 and click **OK**.
5. Click **OK** on the Edit Server Configuration page.
6. Navigate to the Oracle*9i*AS Home page.
7. Select **OC4J\_iFS\_files** and click **Restart**.



## Monitoring Domain, Node, and Service Performance

Use the Oracle Enterprise Manager Web site to monitor domain, node, and service performance. You can use this information to get an overall picture of the domain's performance, or to determine whether the domain's configuration needs modification.

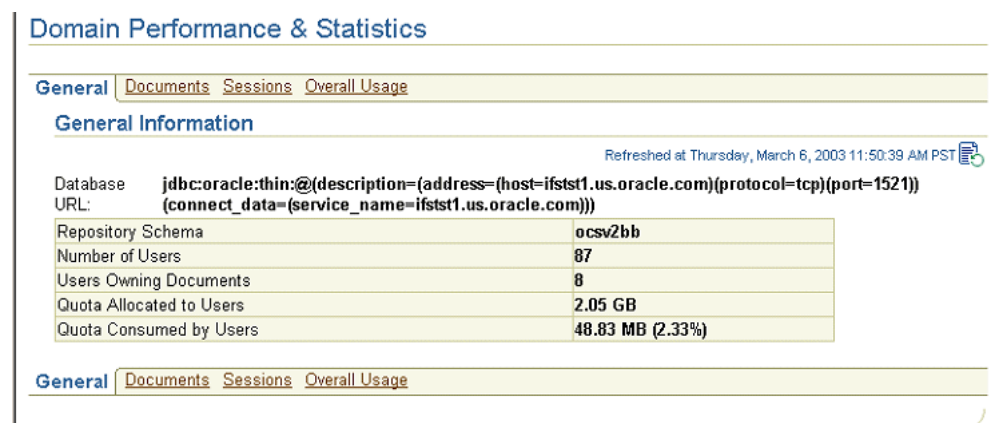
This chapter tells you how to use the Oracle Enterprise Manager Web site to perform these tasks. Topics include:

- [Monitoring Domain Performance](#)
- [Monitoring Node Performance](#)
- [Monitoring Service Performance](#)
- [Viewing Log Files](#)
- [Accessing Metrics and Monitoring Metric Alerts](#)

### Monitoring Domain Performance

1. From the Performance section on the Oracle Files Home page, click **Domain Performance & Statistics**. The Domain Performance & Statistics page appears.

**Figure 7–1 Domain Performance & Statistics Page**



From this page, you can access statistics, usage charts, tables, and summaries to evaluate system performance and guide you in making any necessary changes to your configuration. [Table 7–1](#) lists the various charts, graphs, and tables and

shows you which subtab and view names you should select to access the information.

2. Select one of the four subtabs:
  - The **General** subtab provides general information such as information about document storage and user quota.
  - The **Documents** subtab provides system-wide information about documents.
  - The **Sessions** subtab allows you to view the connected sessions by server type.
  - The **Overall Usage** subtab lets you monitor sessions, threads, and memory by node and host.
3. To refresh the information, click the refresh button on your browser, or click the **Refresh Data** icon in the upper right portion of the page.
4. To navigate between the table view and the chart view, make a selection from the **Select a View** list and click **Go**.

**Table 7–1 Reference to Statistical Information about the Domain and Node**

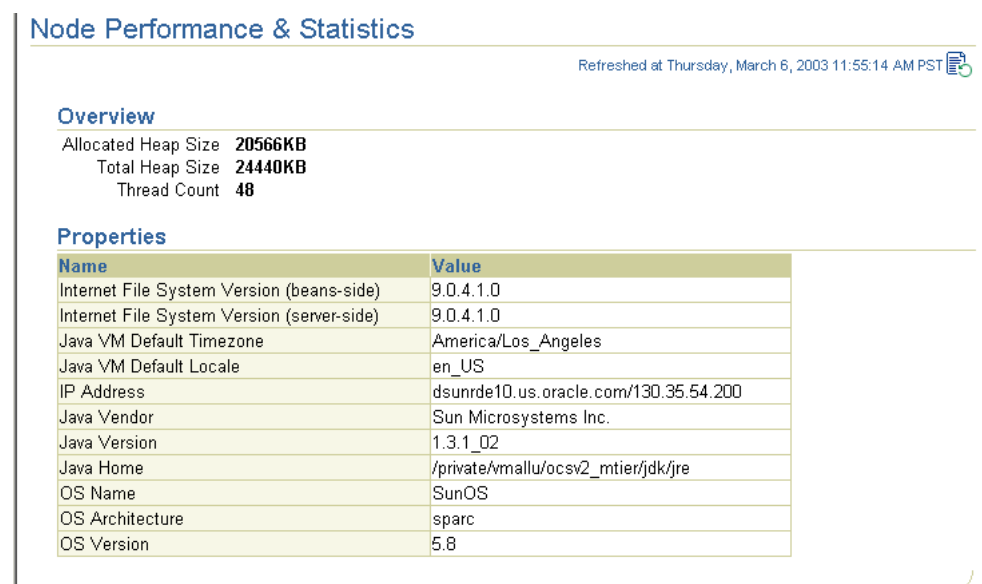
Chart, Graph, or Table Name	Statistics or Information Displayed	Subtab	Select a View Item
General Information	A tabular display listing: <ul style="list-style-type: none"> <li>■ Database URL (connect string) for the database containing the Oracle Files schema where the statistics are calculated</li> <li>■ Schema name for the Oracle Files instance</li> <li>■ Total number of user accounts</li> <li>■ Total users who own documents in the system</li> <li>■ Quota allocated for all users</li> <li>■ Quota consumed by all users</li> </ul>	General	N/A
Document Table	Document distribution and document space consumption.	Documents	Table
Document Distribution Chart	Document distribution 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
Session Table	Tabular display of the total number of connected sessions per protocol server or agent.	Sessions	Table
Session Chart	Pie chart of total number of connected sessions per protocol server or agent. The sessions for all the agents are displayed as a combined result.	Sessions	Chart
Overall Usage Table by Node	Total connected sessions, threads, and memory consumed by each node in the domain.	Overall Usage	Table by Node
Overall Usage Table by Host	Total connected sessions, threads, and memory consumed by each host in the domain.	Overall Usage	Table by Host

**Table 7–1 (Cont.) Reference to Statistical Information about the Domain and Node**

Chart, Graph, or Table Name	Statistics or Information Displayed	Subtab	Select a View Item
Overall Session Usage Chart by Node	Bar graph showing the total number of connected sessions and consumed threads by each node.	Overall Usage	Session Chart by Node
Overall Session Usage Chart by Host	Bar graph showing the total number of connected sessions and consumed threads by each host.	Overall Usage	Session Chart by Host
Overall Memory Usage Chart by Node	Bar graph showing the total amount of memory consumed by each node.	Overall Usage	Memory Chart by Node
Overall Memory Usage Chart by Host	Bar graph showing the total amount of memory consumed by each host.	Overall Usage	Memory Chart by Host

## Monitoring Node Performance

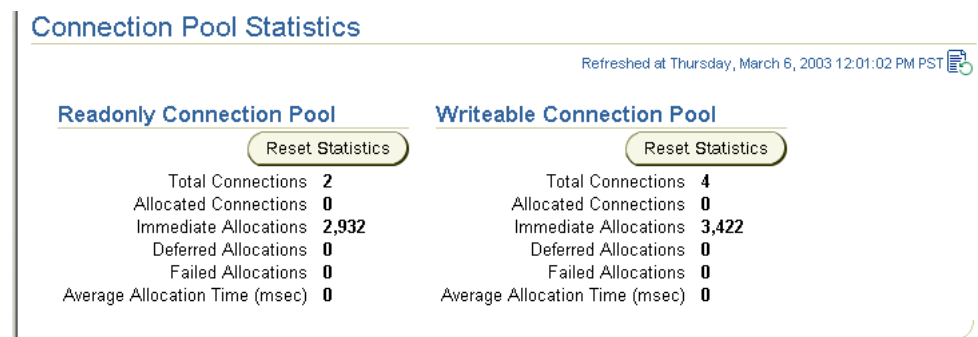
From each Oracle Files Node page, click **Node Performance & Statistics** to display summary-level information about that node.

**Figure 7–2 Node Performance & Statistics Page**

## Monitoring Service Performance

You can view statistical information about 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 Oracle Files 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 7-3 Committed Data Cache Statistics****Figure 7-4 Connection Pool Statistics**

- Click **Reset Statistics** in the Committed Data Cache, Read-Only Connection Pool, or Writeable Connection Pool areas to reset cache or connection pool statistics.

## Viewing Log Files

Read the following sections for information on the Oracle Enterprise Manager Web site, Grid Control, and Oracle Files logs.

### Oracle Enterprise Manager Web Site Logs and Grid Control Logs

The Oracle Enterprise Manager Web site and the Grid Control both generate log files.

- Oracle Enterprise Manager Web site logs are located in:  
`$ORACLE_HOME/sysman/log: em-servlet.log, emd.log, em-application.log`
- If you are using the Grid Control, its logs are located in:  
`$ORACLE_HOME/sysman/log: emoms.log, emoms.trc`

### Oracle Files Logs

Log files are generated by the domain controller and by each node.

- The domain controller log records major state transitions of its nodes (such as started, failed, or restarted) and provides centralized data on overall domain health. The location of the domain controller log cannot be changed. The domain controller log is located in:  
`$ORACLE_HOME/ifs/files/log/transferred_domain_name/DomainController.log`
- The regular node log records the same type of information for each node. This log is useful for troubleshooting protocol servers and agents. All errors are logged

with stack traces. Log file properties, such as Log Level and Rotation Interval, are specified in the node configuration of the node being monitored. By default, the node log is located in:

```
$ORACLE_HOME/ifs/files/log/transferred_domain_name/node_name.log
```

- The HTTP node log records the same type of information for each HTTP node. This log is useful for troubleshooting the Oracle Files application, the WebDAV server, and Oracle FileSync. All errors are logged with stack traces. By default, HTTP node log files are located in:

```
$ORACLE_HOME/j2ee/OC4J_ifs_files/application-deployments/files/OC4J_ifs_files_default_island_1/application.log
```

and

```
$ORACLE_HOME/opmn/logs/OC4J_ifs_files.default_island.1
```

- The `ifsctl` log is located in:
- The Oracle Files Configuration Assistant log is located in:

```
$ORACLE_HOME/ifs/files/log/ifsctl.log
```

```
$ORACLE_HOME/ifs/files/log/FilesConfig.log
```

You can set various options for these log files, such as whether to overwrite the log each time the domain is started, through the domain and node configuration properties. See "[Domain Properties](#)" on page 6-1 and "[Node Configuration](#)" on page 6-3 for more information.

## Accessing Metrics and Monitoring Metric Alerts

If you are using Oracle Enterprise Manager 10g Grid Control, you can access Oracle Files metrics from the Grid Control. The following sections provide information about how to access the metrics and how to set up metric collection:

- [The Grid Control Management Agent](#)
- [Managing Oracle Files with the Grid Control](#)
- [Accessing the Grid Control](#)
- [Changing the Default Metric Collection Behavior](#)
- [Viewing Oracle Files Metrics in the Grid Control](#)
- [Metric Thresholds and Metric Collection Intervals](#)

For more information about the metrics available for Oracle Files, click **Help** on any Grid Control Metrics page. For more information about the Grid Control, see *Oracle Enterprise Manager Concepts*.

### The Grid Control Management Agent

Before you can use the Grid Control to view Oracle Files metrics, you must install a separate Oracle Management Agent in its own Oracle home, and configure it to connect to the Grid Control. To do this, choose the "Additional Management Agent" option in the Oracle Universal Installer. The metrics collected by the Grid Control Management Agent are uploaded to the Oracle Management Service (OMS).

The Management Agent that was installed in the Oracle9iAS Oracle home cannot be used by the Grid Control; instead, it is used by the Oracle Enterprise Manager Web site in that Oracle home. The metrics collected by the Oracle Enterprise Manager Web site Management Agent are consumed by the Oracle Enterprise Manager Web site and are not uploaded to the OMS.

## Managing Oracle Files with the Grid Control

Metric collection is not set up automatically. You must configure Oracle Enterprise Manager to manage Oracle Files. For details on how to do this, see *Oracle Enterprise Manager Managing Oracle Collaboration Suite* on the Oracle Technology Network at:

<http://otn.oracle.com>

## 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`

If the Management Service is running in non-secure mode, access the Grid Control using the Web Cache port. Using the Web Cache port is a prerequisite for self-monitoring. The default port is assigned in the range of 7777-7877. For example:

`http://testcomputer.us.oracle.com:7777/em`

If the Management Service is running in secure mode, access the Grid Control over HTTPS. The default port is assigned in the range of 4443-4543. For example:

`https://testcomputer.us.oracle.com:4443/em`

2. Log in as `sysman`, using the password you specified during Oracle Enterprise Manager installation. Or, log in as another Grid Control user with administrator privileges.

The base target type for Oracle Files is Internet File System.

## Changing the Default Metric Collection Behavior

In some cases, you may want to enable or disable an Oracle Files 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 Files (`oracle_ifs`) targets for the given Oracle Files domain in the Grid Control.

### Reconfiguring Oracle Files (`oracle_ifs`) Targets in the Grid Control

Follow these steps to change the default metric collection behavior of Oracle Files 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 Files 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 Files target and click **Configure**. The target type for Oracle Files is Internet File System.
4. Set the following values to TRUE or FALSE to enable or disable metric collection. The values must be in upper case.
  - **Run Repos Metric?**  
The default is TRUE.
  - **Run Response Time Metric?**  
The default is TRUE. If you set this parameter to TRUE, specify a valid value for **Application URL**. If you sent this parameter to FALSE, enter NULL for **Application URL**.
  - **Run Load Balancer Response Time Metric?**  
The default is FALSE. If you set this parameter to TRUE, specify a valid value for **Load Balanced Application URL**. If you sent this parameter to FALSE, enter NULL for **Load Balanced Application URL**.
5. Click **OK**.

## Viewing Oracle Files Metrics in the Grid Control

After you have logged in to the Grid Control, there are several ways to navigate to the pages that show Oracle Files metrics. Two methods are described in the following sections.

### Using the Groups Subtab

You can use this method to access Oracle Files metrics if you have followed the instructions for setting up groups in *Oracle Enterprise Manager Managing Oracle Collaboration Suite*.

1. From the Grid Control Home page, click the **Targets** tab.
2. Click the **Groups** subtab. A list of groups appears.
3. Select the OCS Group target. The OCS Group Home page appears.
4. Click **Member Targets**. A list of member targets appears.
5. Select the Oracle Files Group target. The Oracle Files Group Home page appears.
6. Click **Member Targets**. A list of member targets appears.
7. Click the name of your Oracle Files middle-tier instance from the list. The name appears in the following format:

```
app_server_host_iFS_db_host:port:service:schema
```

The Oracle Files Grid Control Home page appears. Since the target type for Oracle Files is **Internet File System**, you will see this notation at the top of the page.

8. Click **All Metrics** to see a list of Oracle Files metrics.

### Using the Search Function

To use this method to access Oracle Files metrics, 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 Files host in the **Search** field and click **Go**.
4. Click the name of your Oracle Files instance. The target type is Internet File System.
5. Click **All Metrics** to see a list of Oracle Files 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:

```
$ADDITIONAL_AGENT_ORACLE_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.

---

# Oracle Files Security

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

- [Authentication Using Oracle Internet Directory](#)
- [Protocol Servers](#)
- [Other Security Issues](#)
- [Setting Up Oracle Files to Use SSL](#)
- [Changing the Oracle Files Site Administrator Password](#)
- [Changing the Oracle Files System Password](#)
- [Changing the Oracle Files Schema Password](#)

## Authentication Using Oracle Internet Directory

*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 Files uses Oracle Internet Directory, Oracle's LDAP-compliant directory service, for authentication.

Users supply a credential to the client software. This credential is passed to the Oracle Files protocol servers, which in turn pass it to Oracle Files for authentication. Then, Oracle Files passes the credential to Oracle Internet Directory. Oracle Internet Directory determines whether the credential is valid for the user.

## Protocol Servers

The defined behavior of some industry-standard protocols is inherently insecure. Oracle has no control over the defined behavior of these protocols; these security issues do not represent defects in Oracle software.

## FTP and AFP

The FTP and AFP protocols send unencrypted user passwords across the network. If you are unwilling to accept this behavior, you should disable these protocols. Alternatively, you can configure Oracle Files to require Oracle Files-specific passwords for these protocols to avoid compromising users' Oracle Internet Directory passwords.

## HTTP/DAV

The HTTP/DAV protocol allows both *basic* (plain text) and *digest* (hashed challenge/response) authentication. Oracle Files enables basic authentication by default. If basic authentication is enabled, unencrypted user passwords are sent across the network, unless HTTP/DAV is configured to use SSL. Whether HTTP/DAV uses SSL depends on the configuration of Oracle HTTP Server, and on whether Oracle Files has been configured for SSL. If you are concerned about HTTP/DAV basic authentication, you should configure Oracle HTTP Server and Oracle Files to use SSL.

## Network Channel Encryption

AFP, FTP, HTTP/DAV, NFS, and SMB/NTFS 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, you should disable these protocols, or configure them to use SSL (HTTP/DAV only).

## Oracle Files-Specific Passwords

Some protocols, including AFP and FTP, send unencrypted passwords over the network, which means that if one of these passwords is intercepted, it could provide access to all systems controlled by Oracle Internet Directory for that user. To provide more security, you should create an Oracle Files-specific password (rather than the default Oracle Internet Directory password) to authenticate users of these protocol servers.

The Oracle Files-specific password is stored in Oracle Internet Directory for use with specific protocols. This password is different from and additional to the regular Oracle Internet Directory password.

Each user can have only one Oracle Files-specific password per Oracle Files domain; users cannot create separate passwords for different protocol servers that are in the same domain.

Protocols with which to associate an Oracle Files-specific password were selected during Oracle Files configuration. By default, FTP and AFP require users to log in with an Oracle Files-specific password rather than an Oracle Internet Directory password.

To change the set of protocols that require the Oracle Files-specific password, edit the following service configuration property:

```
IFS.SERVICE.CREDENTIALMANAGER.Oid.IfsPasswordApplications
```

Only the AFP, FTP, and SMB/NTFS protocols may use the Oracle Files-specific password. See ["Changing a Service Configuration"](#) on page 6-8 for information on editing service configuration parameters.

To set Oracle Files-specific passwords, use the Protocol Access page in Oracle Files. See the Oracle Files online help for details.

## Other Security Issues

Read the following sections for security information about administration interfaces, JDBC, Oracle Internet Directory, and client software.

## Administration Interfaces

To perform Oracle Files administration tasks using the Oracle Enterprise Manager Web site or the Grid Control, administrators authenticate using an HTML form. Unless

Oracle HTTP Server and Oracle Enterprise Manager are configured for SSL, unencrypted passwords are transmitted over the network.

## JDBC

By default, JDBC does not encrypt network connections between Oracle Files and the Oracle9i Database Server. Sites can opt to use Oracle Advanced Security to encrypt these connections.

## Oracle Internet Directory

You can choose whether to use SSL to connect to Oracle Internet Directory. If you do not choose to use SSL, unencrypted passwords may be sent over network connections between Oracle Files processes and Oracle Internet Directory.

## Client Software

Oracle FileSync, the client file synchronization software, stores a cookie in the client file system. The Oracle FileSync cookie stores an opaque token (in other words, a randomly-generated string) in order to authenticate a particular user. This credential expires by default after ten days. Administrators can change the expiration date or disable the token credential by changing the `IFS.SERVER.PROTOCOL.DAV.IfsServer.Auth.TokenCredential.Timeout` property. See ["Changing a Server Configuration"](#) on page 6-15 for more information.

## Setting Up Oracle Files to Use SSL

You can configure Oracle Files to use SSL. Before you do this, you must configure Oracle HTTP Server to use SSL. See the *Oracle9i Application Server Security Guide* for information about how to configure Oracle HTTP Server to use SSL.

You can also use SSL to connect to Oracle Internet Directory. Before you do this, Oracle Internet Directory must be configured for SSL. See the *Oracle Internet Directory Administrator's Guide* for detailed information about setting up Oracle Internet Directory for use with SSL.

## Configuring the Oracle Files Application to use SSL

There are two ways to configure the Oracle Files application to use SSL: you can specify SSL settings during Oracle Files configuration, or you can provide SSL settings after Oracle Files has been installed and configured.

### Providing SSL Information During Oracle Files Configuration

During Oracle Files configuration, you must set key values in the Oracle Files Configuration Assistant in order to configure Oracle Files for SSL.

In the Website Information screen, specify one of the following values for **HTTP Port**:

- If you are using Oracle9iAS Web Cache, enter the Web Cache SSL port. This value is typically 4444.
- If you are not using Oracle9iAS Web Cache, enter the non-Web Cache SSL port. This value is typically 4443.

You must also select **Uses SSL** in this screen.

---

---

**Note:** If you are uncertain about which port to specify, use Oracle Enterprise Manager to look at the configuration of the Oracle HTTP Server.

---

---

For full information about using the Oracle Files Configuration Assistant, see the Oracle Files chapter of the *Oracle Collaboration Suite Installation and Configuration Guide*.

## Providing SSL Information Post-Configuration

If you did not provide SSL information during Oracle Files configuration, but still want to set up Oracle Files to use SSL, perform the steps outlined in the following two sections.

**Setting Parameters in Oracle Enterprise Manager Web Site** Use the Oracle Enterprise Manager Web site to set server configuration properties, as follows:

1. From the Oracle9iAS Farm Home page, click the name of the application server on which Oracle Files is running.

The Oracle9iAS Instance Home page appears, listing all the components running on the application server instance. The Oracle Files domain appears in the following format:

`iFS_db_host:port:db_service:files_schema`

2. Click the name of the Oracle Files domain. The Oracle Files Home page appears.
3. Click **Server Configurations** (under the Configuration heading).
4. Click **FilesBaseServerConfiguration**. The Edit page appears.
5. In the Properties section, select **IFS.SERVER.APPLICATION.UIX.Application UseHttps** and click **Edit**.
6. Set the **Value** to True and click **OK**.
7. Select **IFS.SERVER.APPLICATION.UIX.ApplicationPort** and click **Edit**.
8. Set the **Value** to be one of the following:
  - If you are using Oracle9iAS Web Cache, enter the Web Cache SSL port. This value is typically 4444.
  - If you are not using Oracle9iAS Web Cache, enter the non-Web Cache SSL port. This value is typically 4443.
9. Click **OK** on the Edit Property page.
10. Click **OK** on the Edit Server Configuration page.
11. Restart the Oracle Files domain. See ["Starting and Stopping the Oracle Files Domain"](#) on page 5-2 for more information.

**Setting Additional SSL Information** In addition to setting Oracle Files server configuration parameters, you may need to set URLs in Oracle9iAS Portal. Wherever the Files Portlet has been registered in Oracle9iAS Portal, you should update the Files Portlet URLs.

You should also check to see that the SSO server URLs for Oracle Files are set correctly for SSL. To do this, follow these steps:

1. Enter the following URL in a Web browser:

`http://infra_host_name:port/pls/orasso`

where *port* is the Oracle HTTP Server port (typically 7777).

2. Click **Login** and enter `orcladmin` as the user name.
3. Supply the `orcladmin` password and click **Login**.
4. Click **SSO Server Administration**.
5. Click **Administer Partner Applications**.
6. Click the pencil icon that corresponds to the Oracle Files middle-tier computer.
7. Ensure that the **Home URL** appears as follows:  
`https://mid-tier_host:ssl_port`
8. Ensure that the **Success URL** appears as follows:  
`https://mid-tier_host:ssl_port/osso_login_success`
9. Ensure that the **Logout URL** appears as follows:  
`https://mid-tier_host:ssl_port/osso_logout_success`
10. Click **Apply** and confirm to save the changes.

---

**Note:** In steps 7, 8, and 9, *ssl\_port* can be the Web Cache SSL port or the non-Web Cache SSL port, depending on whether you are using Oracle9iAS Web Cache.

---

## Connecting to Oracle Internet Directory Using SSL

There are two ways to set up an SSL connection to Oracle Internet Directory: you can specify SSL settings during Oracle Files configuration, or you can provide SSL settings after Oracle Files has been installed and configured. Before you do this, Oracle Internet Directory must be configured for SSL. See the *Oracle Internet Directory Administrator's Guide* for detailed information about setting up Oracle Internet Directory for use with SSL.

### Providing Oracle Internet Directory SSL Information During Oracle Files Configuration

During Oracle Files configuration, you must set key values in the Oracle Files Configuration Assistant in order to connect to Oracle Internet Directory using SSL.

In the Oracle Internet Directory Login screen, specify the Oracle Internet Directory SSL port in the **Port** field. Typically, the default port number for SSL-enabled Oracle Internet Directory is 636 or 4031. You must also select **Uses SSL** in this screen.

For full information about using the Oracle Files Configuration Assistant, see the Oracle Files chapter of the *Oracle Collaboration Suite Installation and Configuration Guide*.

### Providing Oracle Internet Directory SSL Information Post-Configuration

If you did not provide Oracle Internet Directory SSL information during Oracle Files configuration, but still want to connect to Oracle Internet Directory using SSL, perform the following steps using the Oracle Enterprise Manager Web site:

1. From Oracle9iAS Farm Home page, click the name of the application server on which Oracle Files is running.

The Oracle9iAS Instance Home page appears, listing all the components running on the application server instance. The Oracle Files domain appears in the following format:

```
ifs_db_host:port:db_service:files_schema
```

2. Click the name of the Oracle Files domain. The Oracle Files Home page appears.
3. Click **Service Configurations** (under the Configuration heading).
4. Click the name of the service configuration you are using (for example, **SmallServiceConfiguration**). The Edit page appears.
5. In the Properties section, click **IFS.SERVICE.CREDENTIALMANAGER.Oid.OidSsl**. You may need to move to the second or subsequent page to see this property.
6. Set the **Value** to `true` and click **OK**.
7. Select **IFS.SERVICE.CREDENTIALMANAGER.Oid.OidUrl** and click **Edit**.
8. Change the port number listed in the URL to be the SSL-enabled Oracle Internet Directory port, typically 636 or 4031.
9. Click **OK** on the Edit Property page.
10. Click **OK** on the Edit Server Configuration page.
11. Restart the Oracle Files domain. See ["Starting and Stopping the Oracle Files Domain"](#) on page 5-2 for more information.

## Changing the Oracle Files Site Administrator Password

You cannot change the Oracle Files `site_admin` password in Oracle Internet Directory. Instead, you must change the `site_admin` password in the Oracle Files schema.

To change the Oracle Files `site_admin` password:

1. Log in to the database as the user who owns the Oracle Files schema:

```
sqlplus files_schema/files_schema_password
```

For example:

```
sqlplus ifssys/ifssys
```

2. Execute the following:

```
variable i number;
variable s char(512);
call files_schema$cm.ifsccredentialmanagerpackage.setpassword(
'site_admin', 'new_password', :s) into :i;
print i;
exit;
```

For example:

```
variable i number;
variable s char(512);
call ifssys$cm.ifsccredentialmanagerpackage.setpassword(
'site_admin', 'xxx', :s) into :i;
print i;
exit;
```



A return value of 1 indicates success. Any return value other than 1 indicates failure.

## Changing the Oracle Files System Password

Similar to the `site_admin` password, you cannot change password of the Oracle Files system user in Oracle Internet Directory. Instead, you must change the `system` password in the Oracle Files schema.

To change the password of the Oracle Files system user:

1. Stop the Oracle Files domain. See ["Starting and Stopping the Oracle Files Domain"](#) on page 5-2 for more information.
2. Log in to the database as the user who owns the Oracle Files schema:

```
sqlplus files_schema/files_schema_password
```

For example:

```
sqlplus ifssys/ifssys
```

3. Execute the following:

```
variable i number;
variable s char(512);
call files_schema$cm.ifsccredentialmanagerpackage.setpassword(
'system', 'new_password', :s) into :i;
print i;
exit;
```

For example:

```
variable i number;
variable s char(512);
call ifssys$cm.ifsccredentialmanagerpackage.setpassword(
'system', 'xxx', :s) into :i;
print i;
exit;
```

A return value of 1 indicates success. Any return value other than 1 indicates failure.

4. Start the Oracle Files domain. See ["Starting and Stopping the Oracle Files Domain"](#) on page 5-2 for more information.

After you change the `system` password, you should encrypt it in `targets.xml`. See the following section for more information.

## Encrypting the System Password in targets.xml

The Oracle Files system password is encrypted and stored in Oracle Enterprise Manager, in `targets.xml`. Under certain conditions, such as after an upgrade, you will be prompted to enter the Oracle Files system user name and password when you navigate to the Oracle Files Home page in the Oracle Enterprise Manager Web site. If you see this prompt, you must provide the system user name and password in order to see elements of the Oracle Files domain from the Oracle Files Home page in the Oracle Enterprise Manager Web site.

The Oracle Enterprise Manager Web site will prompt you to enter the `system` user name and password in the following cases:

- After you upgrade the Oracle Files schema.
- After you run `ifscs` to add a second middle tier for an additional HTTP node, regular node, or to migrate the domain controller, and you choose to reuse the existing schema.
- After you have changed the system password in the Oracle Files schema.

If you have performed one of these tasks, you can avoid the system password prompt in the Oracle Enterprise Manager Web site by manually encrypting the system password in `targets.xml`. To do this, follow these steps:

1. Stop the Oracle Enterprise Manager Web site:
  - For UNIX systems, use the `emctl stop` command. You can find the `emctl` command-line tool in `$ORACLE_HOME/bin/`.
  - For Windows systems, stop the Windows service for the Oracle Enterprise Manager Web site.
2. Back up the `targets.xml` file, located in `$ORACLE_HOME/sysman/emd`.
3. Change the system password in `targets.xml`:

- a. Look for the following properties under the `oracle_ifs` target:

```
<property NAME="SysadminUsername" VALUE="system"/>
<property NAME="SysadminPassword" VALUE="password" ENCRYPTED="TRUE"/>
```

- b. If these lines are present, update the `VALUE` attribute of `SysadminPassword` with the new password, and make sure that the `ENCRYPTED` attribute is set to `FALSE`. For example:

```
<property NAME="SysadminPassword" VALUE="test123" ENCRYPTED="FALSE"/>
```

If these lines are not present, insert the two property entries. Specify the appropriate value for `SysadminPassword`, and set the `ENCRYPTED` attribute to `FALSE`.

- c. Save the file.
4. Start the Oracle Enterprise Manager Web site:
  - For UNIX systems, use the `emctl start` command. You can find the `emctl` command-line tool in `$ORACLE_HOME/bin/`.
  - For Windows systems, start the Windows service for the Oracle Enterprise Manager Web site.

When the Oracle Enterprise Manager Web site is started, it encrypts the password in `targets.xml` and changes the `ENCRYPTED` attribute to `TRUE`.

5. Repeat steps 1 - 4 for each middle-tier host in the domain.

## Changing the Oracle Files Schema Password

In addition to the system password, the Oracle Files schema password is also stored in the Oracle Enterprise Manager `targets.xml` file. The password is also stored in Oracle Internet Directory. Follow these steps to change the Oracle Files schema password:

1. Stop the Oracle Files domain using the Oracle Enterprise Manager Web site, or using the `ifsctl stop [domain]` command. You can find the `ifsctl` command-line tool in `$ORACLE_HOME/ifs/files/bin`.

You must also stop the OC4J instances for the HTTP node using the Oracle Enterprise Manager Web site, or using the `opmnctl stopproc gid=OC4J_ifs_files` command. You can find the `opmnctl` command-line tool in `$ORACLE_HOME/opmn/bin`.

See ["Starting and Stopping the Oracle Files Domain"](#) on page 5-2 for more information about stopping the domain and HTTP nodes.

2. Change the schema password for the database user.
3. Change the schema password in Oracle Internet Directory:
  - a. Log in to Oracle Directory Manager.
  - b. In the System Objects directory tree, navigate to the following location:
 

```
Root_Oracle_Context
+ Entry Management
+ cn=OracleContext
+ cn=Products
+ cn=IFS
+ orclApplicationCommonName=domain_name
```
  - c. Click `orclApplicationCommonName=domain_name` to display the Properties tab.
  - d. Enter the new schema password in the **userpassword** field and click **Apply**.
4. Stop the Oracle Enterprise Manager Web site:
  - For UNIX systems, use the `emctl stop` command. You can find the `emctl` command-line tool in `$ORACLE_HOME/bin/`.
  - For Windows systems, stop the Windows service for the Oracle Enterprise Manager Web site.
5. Back up the `targets.xml` file, located in `$ORACLE_HOME/sysman/emd`.
6. Change the schema password in `targets.xml`. If the password is not changed in `targets.xml`, you will not be able to see any regular nodes or HTTP nodes when you browse to the Oracle Files Home page in the Oracle Enterprise Manager Web site.
  - a. Look for the following property under the `oracle_ifs` target:
 

```
<property NAME="SchemaPassword" VALUE="password" ENCRYPTED="TRUE"/>
```
  - b. Update the `VALUE` attribute with the new schema password.
  - c. Make sure that the `ENCRYPTED` attribute is set to `FALSE`:
 

```
<property NAME="SchemaPassword" VALUE="password" ENCRYPTED="FALSE"/>
```
  - d. Save the file.
7. Start the Oracle Enterprise Manager Web site:
  - For UNIX systems, use the `emctl start` command. You can find the `emctl` command-line tool in `$ORACLE_HOME/bin/`.
  - For Windows systems, start the Windows service for the Oracle Enterprise Manager Web site.

When the Oracle Enterprise Manager Web site is started, it encrypts the password in `targets.xml` and changes the `ENCRYPTED` attribute to `TRUE`.
8. Repeat steps 4 - 7 for each middle-tier host in the domain.

9. Restart the Oracle Files Domain using the Oracle Enterprise Manager Web site, or using the `ifscctl start [-v] [-n] [domain]` command. You can find the `ifscctl` command-line tool in `$ORACLE_HOME/ifs/files/bin`.

See ["Starting and Stopping the Oracle Files Domain"](#) on page 5-2 for more information.

10. Stop and then start the OC4J instances for the HTTP node (`OC4J_ifs_files`) on each Oracle Files middle tier.

See ["Starting HTTP Nodes"](#) on page 5-5 for more information.

---

## Maintenance and Tuning

This chapter provides important information about on-going system maintenance, tuning, and recovery. As with any production system, your implementation of Oracle Files should include a basic disaster recovery plan. To manage growth of content in an Oracle Files instance, the system provides some unique capabilities, such as LOB (large objects) file archiving.

This chapter includes the following topics:

- [Backup and Recovery](#)
- [LOB \(Large Objects\) Management](#)
- [Performance Tuning](#)
- [Analyzing Performance Problems](#)

### Backup and Recovery

Planning for failures is one of the most important jobs of any system administrator or DBA. Be sure to implement a daily or weekly backup plan that meets the needs of your business and operations environment. Take advantage of the Oracle database backup capabilities, built right into the database.

Always back up the system before upgrading, migrating new data, or making other major changes. See *Oracle9i Backup and Recovery Concepts* for additional information.

---

**Note:** In addition to the Oracle Files schema, there are three "special" schemas that ensure secure connectivity to other systems. When you back up your system, make sure to include these schemas.

The special schema names are derived from the Oracle Files schema name. For example, if the Oracle Files schema name is IFSSYS, the additional schemas are IFSSYS\$CM, IFSSYS\$DR, and IFSSYS\$ID.

---

### LOB (Large Objects) Management

Oracle Files data is comprised of content and metadata. The majority of data stored in Oracle Files is content and is stored in LOBs (Large Objects) in database tablespaces. All documents are stored as Binary Large Objects (BLOBs), which is one type of LOB provided by the database. See ["Provide Adequate Storage to Improve Performance"](#) on page 9-4 for more information.

Through BLOB management, Oracle Files provides data archiving. Content in the Archive is periodically moved from BLOBs to BFILE. The content is still accessible, and is visible to the Subscriber Administrator.

## Moving Content Off-line or Near-line

As the amount of content stored increases, it may become desirable to move content to a cheaper medium. BFILE support provides off-line and near-line storage.

Oracle Files provides transparent access to content stored as either a BLOB (online storage) or a BFILE (near-line storage). A BFILE is a read-only Oracle data type consisting of a directory object and a filename.

### Moving Content to BFILES

Oracle Files moves content from the Archive to BFILES on a periodic basis. The following two agents control the behavior:

- FilesArchiveFileToBFileAgent
- FilesDelayedArchiveFileToBFileAgent

**Base Path** The file the BFILE points to is located in the database's \$ORACLE\_HOME/ifsfiles/*files\_schema*. UNIX users may configure the real location of the BFILE using symbolic links. Windows users must use this BFILE base path.

**Relative Path** From the base path, the FilesArchiveFileToBFileAgent and the FilesDelayedArchiveFileToBFileAgent associate a relative path. The path now looks like this:

```
$ORACLE_HOME/ifsfiles/files_schema/yyyy/dd/mm/hh/ifsfile_id
```

*ifsfile\_id* is the file naming pattern that associates a unique ID to each piece of content.

---

---

**Note:** If you are using Oracle Collaboration Suite Release 2 (9.0.4.1) or if you have downloaded and applied the Oracle Collaboration Suite Release 2 Patch Set 1 (9.0.4.2.0), the path appears as follows:

```
$ORACLE_HOME/ifsfiles/files_schema/yyyy/dd/mm/hh/mm/ss/ifsfile_id
```

---

---

**Use Symbolic Linking to Change the Storage Location (UNIX only)** You can create a symbolic link to connect the base file location to a different location, such as an HSM system or a tape backup system, rather than limit your BFILE storage to the database's \$ORACLE\_HOME.

### Disabling the BFILE Agents

Some administrators may want to temporarily disable BFILE storage while they formulate an archival strategy and arrange for adequate disk space. To disable BFILE storage, you must ensure that the Oracle Files BFILE agents are not initially started by the node.

To do this, use the Oracle Enterprise Manager Web site to update the node configuration that is used by the node that runs these agents, as follows:

1. From the Oracle*9i*AS Farm Home page, click the name of the application server on which Oracle Files is running. The Oracle*9i*AS Instance Home page appears,

listing all the components running on the application server instance. The Oracle Files domain appears in the following format:

```
ifs_db_host:port:db_service:files_schema
```

2. Click the name of the Oracle Files domain. The Oracle Files home page appears, listing the Domain Controller and nodes that comprise the domain.
3. Click **Node Configurations**, under the Configuration heading.
4. On the Node Configurations page, click the name of the node configuration that is used by the node that runs the BFILE agents. The Edit page appears.
5. Under the Servers heading, select the **FilesArchiveFileToBFileAgent** and click **Edit**.
6. Clear **Initially Started** on the Edit Server page and click **OK**.
7. Under the Servers heading, select the **FilesDelayedArchiveFileToBFileAgent** and click **Edit**.
8. Clear **Initially Started** on the Edit Server page and click **OK**.
9. Click **OK** on the Edit Node Configuration page.
10. Return to the Oracle Files Home page and restart the affected node.

## Performance Tuning

Performance is typically affected by network input/output (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 bottleneck to a new location, so you must approach the tuning task in a logical manner.

The performance tips in this section cover the basics and include:

- [Run the Oracle Files `analyze.sql` Script Frequently](#)
- [Provide Adequate Storage to Improve Performance](#)

See the *Oracle9i Database Performance Tuning Guide and Reference* for complete information.

### Run the Oracle Files `analyze.sql` Script Frequently

Oracle Files uses Oracle9i Database Server's Cost-Based Optimizer (CBO) to determine the most efficient way to execute SQL statements. For the CBO to work properly, the Oracle Files `analyze.sql` script should be run as part of regular Oracle Files operations, especially after large volume changes to the data, such as after users have loaded a large number of files into the instance. This script generates statistics about the distribution of data in Oracle Files so that the CBO can choose the most efficient way to execute SQL statements. For more information about the Cost-Based Optimizer, see the *Oracle9i Database Performance Tuning Guide and Reference*.

Run the script during non-busy periods to avoid impeding performance for users.

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/ifs/files/admin/sql
sqlplus files_schema/password@connect_string @analyze.sql files_schema
```

This script may take a while to run, especially if Oracle Files 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 timestamp. You can query the table for existing saved sets by executing this SQL statement:

```
SQL> select distinct statid from ifs_backup_stats;
```

This query returns a list of all statistics by `statid` (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 your performance was better. For example, if you find that after using the statistics from your 8:00 pm running of `analyze` that performance is worse, then you can restore your statistics from earlier that day using:

```
SQL> @import_backup_stats.sql user_name '08-MAY-02 06:21.40'
```

By restoring the statistics, you are directing the CBO to revert to the way it previously executed SQL statements.

## Provide Adequate Storage to Improve Performance

The largest consumption of disk space occurs on the disks that actually contain the documents residing in Oracle Files, namely the Indexed Medias and Non-Indexed Medias tablespaces. This section explains how the documents are stored and how to calculate the amount of space those documents will require.

### Document Storage and Sizing Issues

BLOBs provide for transactional semantics much like the normal data stored in a database. To meet the criteria of transactional semantics, BLOBs must be broken down into smaller pieces which are individually modifiable and recoverable. These smaller pieces are referred to as chunks. Chunks are actually a group of one or more sequential database blocks from a tablespace that contains a BLOB 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 and consists of the block header, the BLOB header, and the block checksum. Oracle Files configures its BLOBs to have a 32 K chunk size. As an example, assume that the `DB_BLOCK_SIZE` parameter of the database is set to 8192 (8 K). 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 document stored in Oracle Files will consist of some integral number of chunks. Using the previous example, a 500K document will actually use  $512000 / 32528 = 15.74 = 16$  chunks. Sixteen chunks will take up  $16 * 32\text{ K} = 524288$  bytes. The chunking overhead for storing this document would then be  $524288 - 512000 = 12288$



bytes which is 2.4 percent of the original document's size. The chunk size used by Oracle Files is set to optimize access times for documents. Note that small documents, 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 BLOBs is the BLOB Index. Each BLOB index entry can point to eight chunks of a specific BLOB object (NumLobPerIndexEntry = 8). Continuing the example, whereas a 500 K document 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 BLOB space utilization is the PCTVERSION parameter used when creating the BLOB column. For information about how PCTVERSION works, please consult the *Oracle9i SQL Reference*.

Oracle Files uses the default PCTVERSION of 10 percent for the BLOB columns it creates. This reduces the possibility of "ORA-22924 snapshot too old" errors occurring in read consistent views. By default, a minimum of a 10 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, set the PCTVERSION to 1 to reduce disk storage requirements. This may be done at any time in a running system with these SQL commands:

```
alter table odmm_contentstore modify lob (globalindexedblob) (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 BLOB tablespace usage are as follows:

1. Calculate the number of chunks a file will take up by figuring the number of blocks per chunk and 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.

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

For example, if FileSize = 100,000, ChunkSize = 32768, Blocksize = 8192, and BlockOverhead = 60, then Chunks = 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 and then multiplying that result by the PCTVERSION factor. Then add the space for NumLobPerIndexEntry (8) and LobIndexEntryOverhead (46 bytes).

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

Continuing from the preceding example, chunks = 4, ChunkSize = 32768, PctversionFactor = 1.1, NumLobPerIndexEntry = 8, and LobIndexEntryOverhead = 46, so FileDiskSpaceInBytes = 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 these formulas for each file to be stored in the BLOB.

`TableSpaceUsage` = the total of `FileDiskSpaceInBytes` for all files stored

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

### Oracle Files Metadata and Infrastructure

The Oracle Files 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 Oracle Files Primary tablespace. These structures are required to support both the file system and the various protocols and APIs 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.

You should plan for approximately 6 K of overhead per document to be used from this tablespace, or about 2 percent of the overall content. If there is a significant number of custom metadata, such as attributes, subclasses or categories, this overhead should be much larger.

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

## Analyzing Performance Problems

After ensuring that you have run statistics properly and have enough free hard-disk drive to support the tablespaces, you may still have performance problems. If that is the case, you must determine whether the performance bottleneck is caused by the Oracle9i Database Server, by Oracle Files, or by other factors.

To isolate the problem, start by looking at which processes are running and how many resources they are consuming.

1. Run `top` (on UNIX) or 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 the Bottleneck

If the bottleneck is the Oracle shadow process, use the Statspack utility to determine the SQL statement which 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. Additional work must be done to isolate the problem.

For more information about the Statspack utility and Explain Plan, see the *Oracle9i Database Performance Tuning Guide and Reference*.

## If the Java Processes are the Bottleneck

You may have too little memory. For example, if you see any `java.lang.OutOfMemoryError` errors in your log files, increase your Maximum Memory (Xmx) settings for that JVM. For more information about changing the Xmx setting, see the *Oracle Files Planning Guide*.

If users are complaining about 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 Command property of the node configuration. See [Table 6-1, "Node Configuration Properties"](#) on page 6-3 for more information.

In the node log file, output related to garbage collection appears as follows:

```
GC[1] in 305 ms: (6144kb, 6% free) -> (14Mb, 61% free)
```

GC [1] indicates a major garbage collection. GC [0] indicates a nursery space only garbage collection. In this example, the collection took 305 ms. At the start of the collection, heap size was 6144 kb, with 6 percent free. The heap expanded during collection to a 14 Mb heap with 61 percent free.

- In JRE 1.3, major GCs show up as GC [1]. In other JVMs, they may show up as major GC.
  - A major 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 major GCs generally occur more than once every 10 minutes (not just after startup), increase your Xmx settings for that JVM.

### Obtaining Oracle Files Java Cache Statistics

If the bottleneck is an Oracle Files Java process, start by checking the percentage of cache hits for the Oracle Files service. Starting from the Oracle Enterprise Manager Web site Oracle*i*AS Home page ([http://host\\_name:1810](http://host_name:1810)):

1. In the System Components list, click the name of the Oracle Files domain. The Oracle Files Home page appears, listing the components of the Oracle Files installation: Domain Controller, HTTP Node, and Node.
2. Click the name of the node. The Node page appears, showing the current status of the node (Up or Down), the service running and its status, and a list of server objects running on this node.
3. Click the name of the service. Typically, this will be `IfsDefaultService`. The Service page appears.
4. Scroll to the Performance section and click **Committed Data Cache Statistics**. The Committed Data Cache Statistics page appears, showing Cache Size, Cache Puts, Cache Removes, 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.

5. To change the Cache settings for the current session, return to the previous page using the Back button in the browser or the previous link in the path displayed on

the page. In the Configuration section, click **Committed Data Cache Configuration**.

6. Proportionately increase all Cache settings (Cache Capacity, Normal Purge Trigger, Urgent Purge Trigger, Emergency Purge Trigger, Purge Target), and click **Apply** when you are finished.

This will increase your memory usage on the middle-tier computer by approximately 3 KB per object. For example, if you increase cache capacity by 5000, your memory usage will grow by 15 MB.

7. Run the test again, and observe the results.

To make the changes permanent, update the service configuration. See ["Changing a Service Configuration"](#) on page 6-8 for more information.

**Obtaining Oracle Files Connection Pool Statistics** For the Read-Only or Writable connection pool, increase the "Target max. number of connections" and "Absolute max. number of connections" if any of the following is true:

- "Failed allocation" is greater than zero.
- "Total Connections" is more than two higher than "Target max number of connections."
- "Deferred allocations" is greater than 5 percent and "Average time to allocate" is more than 10 milliseconds.

Each additional Target or Absolute connection will use approximately 8 MB per connection on the middle tier and 1 MB per connection on the database.

**Oracle Files Connection Pool Tuning** For the ReadOnly or Writable Connection Pool, increase the "TargetSize" and "MaximumSize" if any of the following is true:

- "FailedAllocationCount" is greater than zero.
- "CurrentSize" is greater than two higher than "TargetSize."
- "DeferredAllocationCount" is greater than 5 percent of "ImmediateAllocationCount" and "AverageAllocationTime" is more than 10 milliseconds.

Note that each additional CurrentSize connection will use approximately 8 MB per connection on the middle tier and 1 MB per connection on the database.

The log file will have connection pool statistics similar to these:

```
Cache performance for S_LibraryObject cache
  CACHESIZE=409
  OBJECTCOUNT=409
  PUTCOUNT=818
  REMOVECOUNT=0
  FINDCOUNT=14617
  HITCOUNT=13949
  MISSCOUNT=668
  HITRATIO=0.9542997879181775
  MISSRATIO=0.04570021208182254
```

```
Cache performance for FolderPath cache
  CACHESIZE=15
  CacheSizeEstimate=15
  ACCESSEQUENCE=599
  SequenceAtLastPurge=0
  PUTCOUNT=15
```

```
REMOVECOUNT=0
PURGECOUNT=0
FINDCOUNT=557
HITCOUNT=433
MISSCOUNT=124
HITRATIO=0.77737881508079
MISSRATIO=0.22262118491921004
```

Cache performance for committed S\_LibraryObjectData cache

```
CACHESIZE=473
CacheSizeEstimate=576
ACCESSSEQUENCE=6821
SequenceAtLastPurge=0
PUTCOUNT=576
REMOVECOUNT=0
PURGECOUNT=0
FINDCOUNT=27092
HITCOUNT=26338
MISSCOUNT=754
HITRATIO=0.972168905950096 <=== THIS IS THE NUMBER TO WATCH
MISSRATIO=0.02783109404990403
```

Cache performance for LibraryObject cache

```
CACHESIZE=221
OBJECTCOUNT=221
PUTCOUNT=221
REMOVECOUNT=0
FINDCOUNT=1473
HITCOUNT=1252
MISSCOUNT=221
HITRATIO=0.8499660556687033
MISSRATIO=0.1500339443312967
```



---

## Customizing Oracle Files

Oracle Files supports several different types of customization. You can change the look and feel of the Oracle Files user interface, and you can define custom workflows to create particular review processes in Oracle Files.

This chapter discusses these different types of customization. Topics include:

- [Branding the Oracle Files User Interface](#)
- [Using Custom Workflows in Oracle Files](#)

### Branding the Oracle Files User Interface

Some organizations have "look and feel" standards (such as the requirement to use a particular company logo or color scheme) within their respective environments. The Web interface for Oracle Files can be customized to match those standards.

System Administrators can make the following customizations to the Oracle Files Web user interface (UI):

- Oracle Files Web UI colors can be changed.
- Oracle Files Web UI fonts can be changed.
- Particular Oracle Files Web UI images (such as the Oracle Files logo) can be modified or replaced.
- The text in the title bar for the Oracle Files Web UI can be changed.

Any changes must be made on each middle-tier deployment of Oracle Files.

---

**Important:** You should make copies of edited files, as all changes will be lost when any patches or upgrades are applied to the Oracle Files software.

---

### Colors

You can change the colors in the Oracle Files Web UI by editing an XML style sheet named `custom.xss`. This file is located in:

```
$ORACLE_HOME/j2ee/OC4J_iFS_files/applications/files/files/cabo/styles/
```

The colors of the Oracle Files Web UI are derived from four defined colors. To change the color scheme, replace one or more of these four colors with colors of your own choosing.

## Fonts

You can change the fonts in the Oracle Files Web UI by editing an XML style sheet, called `custom.xss`, similar to changing Web UI colors. As part of this process, you will need to copy text from another XML style sheet named `blaf.xss`.

Fonts on buttons and images in the Oracle Files Web UI cannot readily be changed.

To change font characteristics in the Oracle Files Web UI:

1. Make a backup copy of `custom.xss` on each of your middle tiers. The `custom.xss` file is located in the following directory:

```
$ORACLE_HOME\j2ee\OC4J_iFS_files\applications\files\files\cabo\styles
```

2. Open `blaf.xss`, located in the following directory:

```
$ORACLE_HOME\j2ee\OC4J_iFS_files\applications\files\files\cabo\styles\
```

3. Copy the following entries from `blaf.xss`:

```
<!-- The default font family -->
<style name="DefaultFontFamily">
  <property name="font-family">Arial,Helvetica,Geneva,sans-serif</property>
</style>

<!-- The default font -->
<style name="DefaultFont">
  <includeStyle name="DefaultFontFamily"/>
  <property name="font-size">10pt</property>
</style>
```

Be careful not to edit this file.

4. Open `custom.xss` and paste in the text from step 3.
5. Modify the two entries as you choose. For example, you could change the entries to the following:

```
<!-- The default font family -->
<style name="DefaultFontFamily">
  <property name="font-family">
    Times New Roman,Arial,sans-serif
  </property>
</style>

<!-- The default font -->
<style name="DefaultFont">
  <includeStyle
    name="DefaultFontFamily"/>
  <property name="font-size">
    9pt
  </property>
</style>
```

6. Save your changes to `custom.xss` on each of your middle tiers.

## Images

You can change particular images/logos in the Oracle Files Web UI by replacing the source images on all Oracle Files middle-tier computers. Oracle Files images are located in the following directory:



```
$ORACLE_HOME/j2ee/OC4J_iFS_files/applications/files/files/static/files
```

Any new image can be used in place of an original image/logo in the Web UI, as long as the new image is the same height and width as the original.

## Title Bar

You can customize the text that appears in the title bar of the Oracle Files Web UI. Any new text for the title bar cannot be localized.

To alter the title bar text, follow these steps:

1. Edit the `FilespageLayout.uit` file, located in the following directory:

```
$ORACLE_HOME/j2ee/OC4J_iFS_files/applications/files/files/WEB-INF/uixsrc/files/
template/pagelayout/
```

2. Look for the following lines:

```
<boundAttribute name = "htmlTitle">
  <concat>
    <dataObject select = "ORACLE_FILES_ONLINE" source = "files:strings"/>
    <fixed text = " - "/>
  </concat>
  <if>
    <dataObject select="isTrain" source="ui:rootAttr"/>
    <messageFormat data:format="title@ui:rootAttr">
      <dataObject select="stageText">
        <if sui:dataObjectListIndex data:index="selectedTrainStep@ui:rootAttr"
          data:value="trainSteps@ui:rootAttr"/>
      </dataObject>
    </messageFormat>
    <dataObject select = "title" source = "ui:rootAttr"/>
  </if>
</boundAttribute>
```

3. Replace:

```
<dataObject select = "ORACLE_FILES_ONLINE" source = "files:strings"/>
```

with the following line:

```
<fixed text = "your_company_name"/>
```

## Limitations on Oracle Files Customizations

The following areas in Oracle Files cannot be customized in Oracle Collaboration Suite, Release 2:

- With the exception of the branding image (logo) and title bar, all other instances of the Oracle Files brand name in the application cannot be modified.
- There is no customized user sign-up in Oracle Files, since the application depends upon Oracle Internet Directory for user information.
- System Administrators can only edit the content on the following pages within the application:
  - Welcome page
  - Help pages
  - FAQ

## Using Custom Workflows in Oracle Files

Oracle Files comes with a default workflow process (also called "review process" in the Oracle Files online help). Although you cannot customize this default process, you can define your own custom workflow process in Oracle Workflow, then register it with Oracle Files.

A *workflow designer*, a person with the necessary skills to design a workflow process in Oracle Workflow Builder, creates the custom workflow process, then the Site Administrator registers the custom workflow process with Oracle Files.

Refer to Chapter 3, "Defining a Workflow Process" in the *Oracle Workflow Guide* for detailed information about creating a custom workflow process definition. You can access the *Oracle Workflow Guide* at the following URL:

<http://otn.oracle.com/pls/db92/db92.docindex?remark=homepage#index-WOR>

Oracle Files must be configured for Oracle Workflow before you can use workflow processes in Oracle Files. For more information, see the *Oracle Collaboration Suite Installation and Configuration Guide*.

### About Custom Workflows

Creating and registering a custom workflow involves the following four steps:

1. **Creating the Workflow Process Definition.** The workflow designer creates a *workflow process definition* (.wft file) using Oracle Workflow Builder. The workflow designer can use the default Oracle Files workflow process (the Review Documents .wft) as an example of a correct, Oracle Files-compliant workflow process definition.

The workflow process definition must handle the following events:

- Launch Event
- Cancel Event
- Response Event

These are the three events that are sent from Oracle Files to Oracle Workflow. Once the workflow designer has created the workflow process definition, he or she uploads the .wft to the workflow schema.

2. **Creating the Launch, Response, and Cancel Events.** The workflow designer creates the launch, cancel and response events.

---

**Note:** Event names cannot be more than 30 characters in length.

---

3. **Creating Event Subscriptions for the Launch, Response, and Cancel Events.** The workflow designer creates event subscriptions for each event.
4. **Registering a Custom Workflow with Oracle Files.** The workflow designer asks the Site Administrator to register the custom workflow process with Oracle Files. The Start Event, Response Event, and Cancel Event must be included in the request.

### Creating the Workflow Process Definition

Oracle Files and Oracle Workflow communicate with one another by sending a series of messages over Advanced Queueing (AQ). First, Oracle Files sends a Launch Event to Oracle Workflow to start the workflow process. Next, Oracle Workflow responds by

sending the URL that Oracle Files needs to access the workflow process status page. After voting is complete (in other words, after the required approvers have responded), Oracle Workflow sends a status message to Oracle Files, indicating whether the status is Approved or Rejected. Finally, Oracle Files sends a Response Event to Oracle Workflow that indicates whether the workflow process concluded successfully, or failed.

If the workflow process expired or was cancelled, Oracle Files sends a Cancel Event to Oracle Workflow.

The following sections provide details on each of these messages in sequence.

### The Launch Event

Oracle Files initiates a new workflow process by sending a Launch Event (message type=Start Event) to Oracle Workflow. To see an example of a Launch Event, refer to `oracle.ifs.files.review`, which is part of the Oracle Files default workflow process.

The Launch Event provides the following parameters:

- **CORRELATIONID:** The workflow process ID.
- **URL[i]:** The URL of the *i*th document being reviewed.
- **NUMDOCS:** The number of documents being reviewed.
- **INITIATOR:** The user who initiated the review process.
- **JUSTIFICATION:** The text justification entered by the initiator.
- **APPROVERS:** Users who must approve the documents, in the format of a space-delimited list of user names.
- **REVIEWERS:** Users who will receive notice that the workflow process has been initiated, in the format of a space-delimited list of user names.

All parameters passed to Oracle Workflow in the Launch Event must be included in all subsequent messages from Oracle Workflow to Oracle Files. For this reason, do not edit the Launch Event.

### The Workflow Process URL

Oracle Workflow must respond to the Launch Event by providing Oracle Files with the URL to access the workflow process status page (message type=PROCESSURL).

Use the following workflow function to retrieve the URL:

```
wf_monitor.GetEnvelopeUrl(wf_core.Translate('WF_WEB_AGENT'),
                           itemtype,
                           itemkey,
                           'NO');
```

The PROCESSURL Event must contain the following parameters:

- **CORRELATIONID:** The workflow process ID.
- **PROCESSURL:** The URL of the workflow process status page. This URL is the one that was returned by the `GetEnvelopeUrl()` function.

---

**Note:** Make sure that the PROCESSURL message includes all the parameters passed to Oracle Workflow in the Launch Event.

---

### The Process Status Event

After voting is complete (i.e., after the required approvers have responded), Oracle Workflow must send a status message to Oracle Files, indicating whether the status is Approved or Rejected (message type=PROCESSSTATUS).

The PROCESSSTATUS Event must contain the following parameters:

- **CORRELATIONID:** The workflow process ID.
- **PROCESSSTATUS:** The status of the workflow process (Approved or Rejected).

---

---

**Note:** Make sure that the PROCESSSTATUS message includes all the parameters passed to Oracle Workflow in the Launch Event.

---

---

### The Response Event

The Response Event is the last message in the workflow process (message type=Response Event). Oracle Files sends the Response Event to Oracle Workflow, indicating whether the workflow process concluded successfully, or failed. To see an example of a Response Event, refer to `oracle.ifs.files.response`, which is part of the Oracle Files default workflow process.

The Response Event provides the following parameters:

- **CORRELATIONID:** The workflow process ID.
- **STATUS:** The final status of the workflow (Success or Failure).
- **EXCEPTION:** The error message that appears if STATUS=Failure.

### The Cancel Event

Oracle Files sends a Cancel Event if the workflow process expired, or was cancelled, on the Oracle Files side (message type=Cancel Event). Oracle Workflow must respond to this event by canceling the corresponding workflow process. To see an example of a Cancel Event, refer to `oracle.ifs.files.cancel`, which is part of the Oracle Files default workflow process.

The Cancel Event provides only one parameter:

- **CORRELATIONID:** The workflow process ID.

## Creating the Launch, Response, and Cancel Events

After the custom workflow process definition is complete, the workflow designer creates the Launch, Response, and Cancel Events in Oracle Workflow. Event names cannot be more than 30 characters in length.

Refer to Chapter 13, "Managing Business Events" in the *Oracle Workflow Guide* for detailed information about creating events in Oracle Workflow.

## Creating Event Subscriptions for the Launch, Response, and Cancel Events

After the Launch, Response, and Cancel events have been created in Oracle Workflow, the workflow designer creates event subscriptions for each of the events:

- The Launch Event and Response Event need to be routed to the uploaded workflow process definition.
- The Cancel Event must send an abort message to the workflow process, using the `wf_engine.AbortProcess()` function.

Refer to Chapter 13, "Managing Business Events" in the *Oracle Workflow Guide* for detailed information about creating event subscriptions in Oracle Workflow.

After creating the event subscriptions, the workflow designer must ask the Site Administrator to register the custom workflow process with Oracle Files, with the Start, Response, and Cancel Event included in the request.

## Registering a Custom Workflow with Oracle Files

The Site Administrator can register a custom workflow process definition on the Registered Workflow Process Definitions page in Oracle Files. Registering the custom workflow process definition will make it available to Workspace Administrators and Participants in a Subscriber.

Site Administrators can register, edit, or delete a custom workflow process definition.

## Registering a Workflow Process Definition

A registered workflow process definition consists of the Workflow Process Definition Name, along with the Launch Event, Response Event, and Cancel Event strings.

To register a custom workflow process definition:

1. Click **Workflow** in Oracle Files.
2. On the Registered Workflow Process Definitions page, enter the **Workflow Process Definition Name**, along with the **Launch Event**, **Response Event**, and **Cancel Event** strings that the workflow designer has provided. The default Oracle Files workflow process definition is registered in the following way:
  - **Launch Event:** `oracle.ifs.files.review`
  - **Cancel Event:** `oracle.ifs.files.cancel`
  - **Response Event:** `oracle.ifs.files.response`
3. Click **Apply** to register the custom workflow process definition for use in Oracle Files.

---

---

**Note:** To add another row, click **Add Another Row**.

---

---

## Editing a Registered Workflow Process Definition

After you have registered a workflow process definition, you can edit its properties. These properties include the Workflow Process Definition Name, along with the Launch Event, Cancel Event, and Response Event strings.

To edit the Registered Workflow Process Definition properties:

1. Click **Workflow** in Oracle Files.
2. From the Registered Workflow Process Definitions page, you can edit one or more Event strings based on the workflow process definition (for **Launch**, **Cancel**, and **Response Events**). The workflow designer provides these strings.

You can also change the **Workflow Process Definition Name**.
3. Click **Apply**. The page refreshes, and your new workflow process definition properties are displayed.

---

---

**Note:** If you cannot cancel a workflow process, then the Cancel Event registered with Oracle Files is not consistent with the Cancel Event string in the workflow process definition in Oracle Workflow. Edit the Oracle Files Cancel Event to solve the problem.

---

---

### Deleting a Registered Workflow Process Definition

When a Registered Workflow Process Definition is deleted, any pending processes using that definition are canceled.

To delete a Registered Workflow Process Definition:

1. Click **Workflow** in Oracle Files.
2. From the Registered Workflow Process Definitions page, click the **Trash** icon in the **Delete** column that corresponds to the Registered Workflow Process Definition you want to remove.
3. Click **Apply**. The deleted Registered Workflow Process Definition is not displayed, and is no longer available to Subscribers.

## Setting Up E-Mail Notifications in Oracle Workflow

In order to configure Oracle Workflow to send e-mail notifications, you must perform the following tasks:

- Set up UNIX Sendmail
- Set up the Oracle Workflow Notification Mailer
- Create a configuration file for the Oracle Workflow Notification Mailer
- Start the Oracle Workflow Notification Mailer

---

---

**Note:** Only instructions for UNIX and Linux are currently available.

---

---

### Setting Up UNIX Sendmail

If you want to use UNIX Sendmail for Oracle Workflow email notifications, you must ensure that Sendmail is configured on the operating system so that users can send e-mail to external recipients, as well as receive e-mails from them.

To determine if Sendmail is running:

1. Log on to the middle-tier host where Oracle Workflow is installed as the "workflow" user.
2. Type the following command in a UNIX shell prompt:

```
ps -ef | grep sendmail
```

If Sendmail is running, it returns a valid Sendmail process.

To start Sendmail if it is not running:

1. Type the following command to start Sendmail:

```
/usr/sbin/sendmail -bd -q15m
```

The location of the Sendmail binary can vary depending on your operating system configuration.

To test if Sendmail is configured correctly:

1. Type the following commands:

```
telnet localhost 25
helo localhost
mail from : <>
```

You must get a response of "Sender OK."

2. Next, type the following:

```
rcpt to : <email_address_of_recipient>
```

You must get a response of "Recipient OK."

3. Next, type the following:

```
data
subject : xxx
yyy
zzz
.
quit
```

---

**Note:** You must type a period to mark the end of the e-mail body.

---

4. Check whether the recipient receives the e-mail. If the recipient receives the e-mail, then Sendmail is configured correctly.

### Setting Up the Oracle Workflow Notification Mailer

Set up the Oracle Workflow Notification Mailer on the middle-tier host where Oracle Workflow is installed.

1. Create a UNIX account for Oracle Workflow (for example, "Workflow"). This UNIX account should only receive Workflow mail.
2. Ensure that the environment for the Workflow UNIX user to run the Notification Mailer is set up in the same way as the environment for the user who installed Oracle Workflow.
3. Add the Workflow UNIX user to the dba group in the operating system, and set the umask for the account as 022.
4. Set PATH to sendmail binary.
5. Set LD\_LIBRARY\_PATH to \$ORACLE\_HOME/lib (if not already set).
6. Check that the Workflow UNIX user can log in to the server, and ensure that e-mail can be sent to and received from external recipients through Sendmail.
7. Ensure that the Workflow UNIX user can log in to the Oracle database server. You can check this by using SQL\*Plus to log in to the database as the Workflow database user:

```
sqlplus workflow_schema/password@connect_string
```

The *workflow\_schema* is typically owf\_mgr.

8. Ensure that the Workflow UNIX user has the necessary permissions for the following three files:

- **The Notification Mailer program.** The program file, `wfmail.snd`, is located in `$ORACLE_HOME/bin`.
- **The Notification Mailer tag file.** The tag file, `wfmail.tag`, is located in `$ORACLE_HOME/wf/res`.
- The sample configuration file. The configuration file, `wfmail.cfg`, is located in `$ORACLE_HOME/wf/res`.

### Creating a Configuration File for the Oracle Workflow Notification Mailer

You must create a configuration file for the Oracle Workflow Notification Mailer. Edit the sample configuration file, `wfmail.cfg`, located in `$ORACLE_HOME/wf/res`.

The content of the configuration file is formatted as follows:

```
#Description
PARAMETR1=value_1
```

```
#Description
PARAMETR2=value_2
```

Edit the following parameters in the `wfmail.cfg` file:

- **CONNECT.** Connection information for the database account where Oracle Workflow server is installed, in the following format:

```
user_name/password@connect_string
```

- **ACCOUNT.** Connection information for the mail account that the program uses to send notification messages. For Sendmail, the account information would be the full path of the mail spool file where the incoming messages are stored, such as:

```
/var/mail/Workflow_UNIX_user_account
```

For example:

```
/var/mail/Workflow
```

- **REPLYTO.** A default reply-to e-mail address, if the e-mail account that processes responses is different from the e-mail account that sends outgoing notifications. For example:

```
some_admin@yourDomainName
```

- **HTMLAGENT.** The base URL that identifies the HTML Web Agent that handles HTML notification responses. This URL is required to support e-mail notifications with HTML attachments. The format is:

```
http://server_name:portID/pls/new_workflowDAD
```

For example:

```
http://myserver:8799/pls/ocs_wf
```

- **TAGFILE.** The full path and name of the Oracle Workflow tag file:

```
ORACLE_HOME/wf/res/wfmail.tag
```

Replace `ORACLE_HOME` with the actual Oracle home directory. Do not type `$ORACLE_HOME`.

- **HTML\_MAIL\_TEMPLATE.** The Workflow approval and rejection mail template.



If you are using Sendmail, do not set this parameter. If you want to use a mail transfer agent other than Sendmail (for example, the Oracle Collaboration Suite mail transfer agent), make sure to set this parameter as follows:

```
OPEN_MAIL_OUTLOOK
```

All other parameters take the default values.

### Starting the Oracle Workflow Notification Mailer

After you have set up the Oracle Workflow Notification Mailer and created a configuration file, you should run the Notification Mailer in the background. Follow these instructions to keep the Notification Mailer running even after the Workflow UNIX account has logged out, and to record standard output and error messages separately:

- As the Workflow UNIX user, enter the following single line:

```
nohup $ORACLE_HOME/bin/wfmail.snd -f $ORACLE_HOME/wf/res/wfmail.cfg  
1>mailer.log 2>mailer_err.log &
```

- Since the password parameter in the \$ORACLE\_HOME/wf/res/wfmail.cfg file is in Cleartext and poses a security problem, you can start the Notification Mailer without specifying the CONNECT parameter in the configuration file:

```
nohup $ORACLE_HOME/bin/wfmail.snd -f $ORACLE_HOME/wf/res/wfmail.cfg owf_  
mgr/password@connect_string 1>mailer.log 2>mailer_err.log &
```

---

**Note:** Even this method of running the Oracle Workflow Notification Mailer is not entirely secure, since anyone with access to the middle tier could type `/usr/ucb/ps -auxwww | grep wfmail.snd` to get the CONNECT information.

---



# Troubleshooting

This chapter provides the following information:

- [Troubleshooting General Problems](#)

## Troubleshooting General Problems

This section contains information to assist with general problems and performance issues. The probable cause and a corrective action are provided for each problem.

**Table 11–1 Troubleshooting General Problems**

Problem	Probable Cause	Corrective Action
An out-of-memory exception is raised when running Oracle Files.	The maximum Java heap size is too low.	Increase the heap size by modifying the <code>-Xmx</code> setting for that node configuration. See the <i>Oracle Files Planning Guide</i> for more information.
Server is generally slow for read and write activity.	Probable cause #1: Server memory is overcommitted. The server is excessively swapping memory blocks to disk.	Run system monitoring tools, such as <code>vmstat</code> (UNIX) and look for excessive page swapping to verify the problem.  Adjust the following parameters in your database's <code>init.ora</code> file: <ul style="list-style-type: none"> <li>■ Reduce <code>processes</code>.</li> <li>■ Reduce <code>open_cursors</code>.</li> <li>■ Reduce <code>db_block_buffers</code>.</li> </ul> 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 Files server into a two-tier configuration.  For more information on adjusting the parameters in the <code>init.ora</code> file, see the <i>Oracle Collaboration Suite Installation and Configuration Guide</i> .
	Probable cause #2: CTXHX is using 100 percent of your CPU.	See <a href="#">Appendix A, "Oracle Text Reference"</a> .
Server is slow only on read or search activity.	Large volumes of data have been loaded but the CBO statistics weren't updated.	If the Oracle9i Cost-Based Optimizer is using stale statistics data, performance suffers. Run the <code>analyze.sql</code> script located in the <code>\$ORACLE_HOME/ifs/files/admin/sql</code> directory to refresh the statistics.
Server is slow only on content-based search activity.	Probable cause #1: Oracle Text tablespaces are on the same disk as other database files.	Move the Oracle Text tablespaces to other disks. See the <i>Oracle Collaboration Suite Installation and Configuration Guide</i> and the <i>Oracle9i Database Administrator's Guide</i> for more information on moving tablespaces.
	Probable cause #2: Oracle Text indexes have become fragmented.	Regularly optimize the Oracle Text Oracle index <code>IFS_TEXT</code> . See <a href="#">"Maintaining the IFS_TEXT Index By Using the Oracle Text PL/SQL Packages"</a> on page A-2 for more information.

**Table 11–1 (Cont.) Troubleshooting General Problems**

Problem	Probable Cause	Corrective Action
Server is slow only on write activity.	Probable cause #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 the <i>Oracle9i Database Administrator's Guide</i> for more information. In general, Redo logs should be switching every hour or less frequently. See the <code>\$ORACLE_HOME/rdbms/sid/bdump</code> directory for the latest logs which indicate the frequency of Redo log switching.
	Probable cause #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 the <i>Oracle9i Database Administrator's Guide</i> and the <i>Oracle9i Database Performance Tuning Guide and Reference</i> 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 above, 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.
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 A-2 for more information.
Problems with outbound FTP on UNIX.	You are using <code>/usr/bin/ftp</code> on UNIX and the default port number in <code>/etc/services</code> 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.
Problems with NFS on AIX, HP-UX, or Compaq Tru64 platforms.	You are trying to run multiple NFS servers on these platforms.	On AIX, HP-UX, and Compaq Tru64 platforms, the Oracle Files NFS server must use the primary NFS port (2049). Because of this, you cannot run both the native UNIX NFS server and the Oracle Files NFS server on these platforms.
Want to reset the Oracle Files system password without knowing what it is.	Have forgotten the Oracle Files system password.	See "Changing the Oracle Files System Password" on page 8-7.
The administrator has uploaded files and removed them and doesn't 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 Oracle Enterprise Manager Web site to look at the Initial Time of Day and Activation Period entries for the Content Garbage Collection Agent.  Also check the <code>Node.log</code> and see if the Content Garbage Collection Agent is getting activated at the periodic intervals.
Cannot access Oracle Files from outside the firewall using SMB.	The required port is not open.	Windows clients can only access SMB if it is running on port 139, so you will need to open up port 139 to the external computer.
Accessing Oracle Files from outside the firewall using SMB is very slow.	SMB is inherently slow over the Internet.	Because the SMB protocol frequently sends hundreds of network requests for each user operation, using SMB over any network with high latency, such as the Internet, might be too slow for end users. Oracle recommends using SMB only if the end user is within 100 miles of the Oracle Files server. See the <i>Oracle Files Planning Guide</i> for more details.
Users fail to be provisioned, or newly provisioned users cannot be added to workspaces.	Required user attributes were not set in Oracle Internet Directory.	The following Oracle Internet Directory user attributes must be non-null for all users: <code>sn</code> , <code>givenName</code> , <code>mail</code> . In addition, all users must have a non-null username.  The username is specified by the <code>orclCommonNicknameAttribute</code> in the Subscriber's OracleContext. See the <i>Oracle Internet Directory Administrator's Guide</i> for more information on viewing the <code>orclCommonNicknameAttribute</code> .
"503 Service Unavailable" error message.	The OC4J instance was not restarted after starting the Oracle Files Domain.	<ol style="list-style-type: none"> <li>1. If the domain is not started, run <code>ifscctl start</code>.</li> <li>2. From <code>\$ORACLE_HOME/opmn/bin/</code>, run <code>opmnctl restartproc gid=OC4J_ifs_files</code>.</li> <li>3. Check the HTTP Node log file to ensure that the HTTP node has started.</li> </ol>

**Table 11–1 (Cont.) Troubleshooting General Problems**

Problem	Probable Cause	Corrective Action
Cannot log in to FTP.	Protocol Access is not enabled for that user.	Log in to Oracle Files with the user account that cannot access FTP and go to the Protocol Access page, where you can set an Oracle Files-specific password. You can then log in to FTP using the Oracle Files-specific password.
When using NTFS, nothing gets written into the node log.	The Log Level of the node configuration is not set high enough.	NTFS will not write into the node log unless the Log Level is set to 6. See " <a href="#">Changing a Node Configuration</a> " on page 6-3 for information about how to set the Log Level.
Oracle Files domain link is not active in the Oracle Enterprise Manager Web site.	Did not restart Oracle Enterprise Manager after Oracle Files configuration.	Restart Oracle Enterprise Manager. See <a href="#">Table 4–1, "Starting and Stopping the Oracle Enterprise Manager Process"</a> on page 4-3 for more information.
Cannot connect to Oracle Files.	The Oracle Files server may be using DHCP.	If Oracle Files is using DHCP, use the server's current IP address to connect rather than the hostname. All Oracle Files protocols are affected, including HTTP.
Oracle Files protocols fail to establish new connections after 10,000+ connects/disconnects.	You are using a 9.0.2x version of Oracle9iAS Infrastructure on a Linux, Windows, or Tru64 platform.	Apply the appropriate ARU patch for your platform and Infrastructure version number. See Note 252888.1 on Oracle <i>MetaLink</i> for a full description of this problem, including the patch IDs. You can access Oracle <i>MetaLink</i> at: <a href="http://metalink.oracle.com">http://metalink.oracle.com</a>



---

## Oracle Text Reference

Oracle Files 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 Files (IFS\_TEXT). In addition, the end user's experience of the performance of the search can depend on how much time you let elapse before an in-progress search times out.

This appendix provides information about how to maintain the Oracle Text index to ensure optimal Oracle Files 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 interMedia 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 interMedia-related nomenclature. For example, the database schema that owns all Oracle Text objects, such as the indexes, is CTXSYS.

For detailed information about Oracle Text, visit the Oracle Technology Network (<http://otn.oracle.com/products/text/>).

### Oracle Text Tablespaces and Disk Utilization

Disk space for Oracle Text is divided among three distinct tablespaces:

- The **Oracle Text Data** tablespace 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 Keymap** tablespace contains the tables and indexes required to translate from the Oracle Files locator of a document (the Oracle Files 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 per indexed document.

- The **Oracle Text Index** tablespace contains the B\*tree database index that is used against the text token information stored in the Oracle Text Data tablespace. This will grow as a function of the ASCII content just as the Oracle Text Data 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.

Use this information to estimate and plan disk storage needs for your Oracle Files instance.

## Creating and Maintaining the Oracle Text Index

At the end of the configuration process for Oracle Files, the Oracle Files Configuration Assistant uses the SQL scripts shown in [Table A-1](#) to create and populate the IFS\_TEXT index.

These scripts are located in the following directory:

```
$ORACLE_HOME/ifs/files/admin/sql
```

If the installation process fails and you need to run these scripts manually, you should execute the scripts at a SQL\*Plus prompt after logging on as the Oracle Files schema user (for example, IFSSYS).

**Table A-1 SQL Scripts for Creating Oracle Text Index**

Script	Usage
CreateContextFunnelProcedure.sql	Creates the procedure used by USER DATASTORE.
GrantContextToIFS.sql	Grants the Oracle Files user (schema) privileges on the Oracle Text-specific commands required to maintain the index.  You must run this script as a database user with administrator privileges, such as SYSTEM.
CreateContextPreferences.sql	Tablespace and other text preferences are created by the Oracle Files user.
CreateContextIndex.sql	Creates the IFS_TEXT index based on the text preferences.

## 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, but adds and deletes records that have changed since the last synchronization. Since 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 Files configuration, the procedures to sync and optimize the IFS\_TEXT index are automatically set up to run periodically in the background, using the DBMS\_JOBS package of the Oracle9i Database Server. DBMS\_JOBS procedures, which are similar to cron jobs on UNIX systems, are portable across all platforms on which the Oracle9i Database Server runs.

When the Oracle Files schema is created during configuration, two DBMS\_JOBS are set up: Sync Job and Optimize Job.

---

**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 automatically.

---

### 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 is set up to run 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 one hour allocated for the optimization task. The job is set up to run every 24 hours, starting at midnight.

### Monitoring DBMS\_JOBS

DBMS\_JOB log files can be found under the Oracle home that hosts the Oracle9i Database Server, 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 at any given time 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 Files schema using SQL\*Plus.

### Changing or Removing the Default DBMS\_JOBS

Two SQL files are used to set up and clear DBMS\_JOBS in Oracle Files: SetupContextJobs.sql and ClearContextJobs.sql. These files are located in the following directory:

```
$ORACLE_HOME/ifs/files/admin/sql
```

SetupContextJobs.sql is used by the system during configuration to set up Sync Job and Optimize Job. ClearContextJobs.sql is provided for you to remove Sync Job and Optimize Job, in case you want to set up your own DBMS\_JOBS.

See the *Oracle9i 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 Files schema user, and enter:

```
exec ctx_ddl.sync_index('ifs_text');
```

You can also run the SyncContextIndex.sql script from the \$ORACLE\_HOME/ifs/files/admin/sql directory. In addition to synchronizing the IFS\_TEXT index, this script will print extra log information to the console.

To optimize an existing IFS\_TEXT index, use SQL\*Plus to connect as the Oracle Files schema user, 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 Files Documents

Oracle Files provides some utility-type SQL scripts to facilitate interaction with Oracle Text (see [Table A-2](#)). Read each .sql file for additional usage details. All scripts are available in:

```
$ORACLE_HOME/ifs/files/admin/sql
```

**Table A-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 call to <code>ctx_output.add_event()</code> , to monitor on a rowid by rowid basis.
ViewDocumentByRowID.sql	Script that enables you to view additional information about a document that is indexed by Oracle Text. Use the <code>docid</code> from the Oracle Text log with this script.

## Indexing Non-Standard Content Types

Oracle Files 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 Oracle Enterprise Manager Web site. The MIME type of a document is determined by its extension.

For example, you may want to index all your .java source code files. To do so:

1. Use the Oracle Enterprise Manager Web site to add the .java MIME type and designate it as Indexed on the New Format page.
2. Insert the files into the repository.
3. Sync the index using the procedure discussed in ["Manually Synchronizing and Optimizing IFS\\_TEXT"](#) on page A-4.

## 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. Increase this value and 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.

## Troubleshooting Oracle Text Problems

This section provides Oracle Text troubleshooting information.

**Table A-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 make sure that the Oracle Text indexing jobs are running. See <a href="#">"Creating and Maintaining the Oracle Text Index"</a> on page A-2 for more information.
Server is slow only on content-based search activity.	Probable cause #1: Oracle Text tablespaces are on the same disk as other database files.	Move the Oracle Text tablespaces to other disks. See the <i>Oracle9i Database Administrator's Guide</i> for more information on moving tablespaces.
	Probable cause #2: Oracle Text indexes have become fragmented.	Regularly optimize the Oracle Text index <code>GLOBALINDEXEDBLOB_I</code> . See <a href="#">"Manually Synchronizing and Optimizing IFS_TEXT"</a> on page A-4 for more information.
Searching on the contents of new documents stops working.	A recent document has caused Oracle Text server to fail.	<ol style="list-style-type: none"> <li>1. Log in to SQL*Plus as <code>files_schema/schema_password</code>, and enter the following command:  <pre>select count(*) from ctx_user_pending;</pre> </li> <li>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 Files documents these rows refer to, see the problem <a href="#">"Oracle Files rows show up in the Oracle Text view ctx_user_index_errors."</a></li> <li>3. Check again to see if there are any rows in <code>ctx_user_pending</code> and, if so, that the rows are changing.</li> <li>4. If this does not resolve the issue, contact your Oracle Support Representative for further assistance.</li> </ol>

**Table A–3 (Cont.) Troubleshooting Oracle Text Problems**

Problem	Probable Cause	Corrective Action
Oracle Files rows show up in the Oracle Text view <code>ctx_user_index_errors</code> .	Oracle Files documents are corrupt or do not have the correct extension.	<ol style="list-style-type: none"> <li>Determine which Oracle Files document is being referred to, based on the <code>err_textkey</code> from <code>ctx_user_index_errors</code>.   <code>SQL*Plus files_schema/schema_password</code>   <pre> select du.uniquename, vd.name, co.contentsize, cs.id, vd.id from odm_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 = <b>err_textkey</b> ) order by cs.id;</pre> </li> <li>Go to the Oracle Files Web interface and log in as the Subscriber Administrator.</li> <li>Search on the document name <code>vd.id</code>, where <code>vd.id</code> is the <code>vd.id</code> returned from the select statement above.</li> <li>Check document attributes, such as document size, to make sure that it is the correct document.</li> <li>Examine this document, looking for these problems: Is the file damaged in any way? Is the file name extension correct for this document? Is the character set of the document correct?</li> <li>If no obvious problems are found, send the document to your Oracle Support Representative for further diagnosis.</li> </ol>
Oracle Files rows never get processed and never leave the Oracle Text view <code>ctx_user_pending</code> .	Oracle Files documents are corrupt or do not have the correct extension.	<ol style="list-style-type: none"> <li>Follow the steps in "Oracle Files rows show up in the Oracle Text view <code>ctx_user_index_errors</code>." to determine which Oracle Files documents are being referred to, substituting <code>ctx_user_pending</code> for <code>ctx_user_index_errors</code> and <code>pnd_rowid</code> for <code>err_textkey</code>.</li> <li>Examine this document, looking for these problems: Is the file damaged in any way? Is the file name extension correct for this document? Is the character set of the document correct?</li> <li>If no obvious problems are found, send the document to your Oracle Support Representative for further diagnosis.</li> <li>Delete the document from Oracle Files.</li> </ol>

## Service Configuration Reference

An Oracle Files 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.

---

**Note:** Spaces can be included in service configuration properties. For this reason, do not use spaces to separate alternate values of a property. You must use a comma as a delimiter.

---

**Table B–1** IFS.SERVICE.\* Properties

Property	Description and Usage Note	Default	Required?
IFS.SERVICE. DefaultCharacterSet	Default character set, in IANA format, for Oracle Files Subscribers. Can be overridden on a per-session basis. Default character set for each user is determined by the user's Primary User Profile.	Character set of the database instance ISO-8859-1	No
IFS.SERVICE. DefaultLanguage	Default language, as an Oracle language name, for Oracle Files Subscribers. Can be overridden on a per-session basis. Default language for each user is determined by the user's Primary User Profile.	Based on configuration.	No
IFS.SERVICE. MaximumConcurrentSessions	Maximum number of sessions the service can support concurrently. Default of 0 means unlimited.	0	No
IFS.SERVICE. MaximumConcurrentSessionsPerUser	Maximum number of sessions per user the service can support. Default of 0 means unlimited. If set to other than 0 and maximum is exceeded, service throws IFS-20132 error.	0	No

**Table B–1 (Cont.) IFS.SERVICE.\* Properties**

Property	Description and Usage Note	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 session's resources.) Default is 60 seconds between checks. Set to 0 to disable the checking.	60	No
IFS.SERVICE. SessionOperationTimeoutPeriod	Number of seconds after which certain Oracle Files API calls are terminated, even if incomplete. If an operation times out in this manner, it is terminated, its transaction is aborted, and an exception is thrown. The session performing the operation remains valid. Set to 0 to disable session operation timeout.	300	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. 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 Files repository.  Set to 0 to disable heartbeat.	60	No
IFS.SERVICE. PollForEventsFromOtherServices Period	Seconds between checks for incoming events from other services. Set to 0 to disable inter-service event polling.	2	No
IFS.SERVICE. TransportEventsToOtherServices Period	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. 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. 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. 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
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. PurgeTarget	The target cache size, in ACLs, upon completion of a purge cycle. Must be less than IFS.SERVICE.ACLCACHE.NormalTrigger.	400 - Small 1600 - Medium 4000 - Large	No

**Table B-1 (Cont.) IFS.SERVICE.\* Properties**

Property	Description and Usage Note	Default	Required?
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.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 20 - Medium 30 - Large	No
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 40 - Medium 60 - 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.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 be thrown.	10000	No
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.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 20 - Medium 30 - Large	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 40 - Medium 60 - 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

**Table B-1 (Cont.) IFS.SERVICE.\* Properties**

Property	Description and Usage Note	Default	Required?
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 be thrown.	10000	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.IfsPasswordApplications, IFS.SERVICE.CREDENTIALMANAGER.Oid.OidSsl, and IFS.SERVICE.CREDENTIALMANAGER.Oid.OidUrl.	N/A	N/A
IFS.SERVICE.CREDENTIALMANAGER.Oid.IfsPasswordApplications	The names of the applications that authenticate using users' Oracle Files-specific passwords instead of their Oracle Internet Directory passwords.	FtpServer AfpServer	No
IFS.SERVICE.CREDENTIALMANAGER.Oid.OidSsl	Whether Oracle Files 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
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, upon completion of a purge cycle. Must be less than IFS.SERVICE.DATACACHE.NormalTrigger.	4000 - Small 16000 - Medium 40000 - Large	No



**Table B–1 (Cont.) IFS.SERVICE.\* Properties**

Property	Description and Usage Note	Default	Required?
IFS.SERVICE.JDBC.DatabaseUrl	URL of the database instance containing the Oracle Files schema JDBC connect string. See the <i>Oracle9i JDBC Developer's Guide and Reference</i> for syntax and examples.	none	No
IFS.SERVICE.JDBC.DriverType	Specifies the JDBC driver type. Do not change.	oci8	No
IFS.SERVICE.JDBC.TracingEnabled	Prints JDBC debugging information to the standard output. Do not change.	false	No
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.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 session's "heartbeat." Must be either <code>oracle.ifs.beans.LibrarySessionEventPollerThreadPerProcess</code> (recommended) or <code>oracle.ifs.beans.LibrarySessionEventPollerThreadPerSession</code> .	<code>oracle.ifs.beans.LibrarySessionEventPollerThreadPerProcess</code>	No
IFS.SERVICE.SESSION.EventPollerPeriod	The period, in milliseconds, of the session's "heartbeat." In addition to indicating the session's health 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 is thrown. The session performing the search remains valid. A value of 0 disables search time-outs.	60	No
IFS.SERVICE.SESSION.BEANSOBJECTCACHE.Size	The target maximum size of the "bean-side" session object cache, in <code>LIBRARYOBJECTS</code> . The bean-side session object cache holds instances of <code>oracle.ifs.beans.LibraryObject</code> . If <code>IFS.SERVICE.SESSION.SERVEROBJECTCACHE.IsUnbounded</code> is false, this value is ignored and implicitly equal to <code>IFS.SERVICE.SESSION.SERVEROBJECTCACHE.Size</code> .	750	No
IFS.SERVICE.SESSION.FOLDERPATHCACHE.Enabled	Whether the session caches the resolution of folder paths.	true	No
IFS.SERVICE.SESSION.FOLDERPATHCACHE.Size	The absolute maximum size of the session's folder path cache, 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

**Table B-1 (Cont.) IFS.SERVICE.\* Properties**

Property	Description and Usage Note	Default	Required?
IFS.SERVICE.SESSION.FOLDERPATHCACHE.UrgentTrigger	The cache size, in folder paths, at which the session's folder path cache 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, upon 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, upon 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. Refer to the Javadoc for class oracle.ifs.common.TraceLogger for a list of Oracle-defined channels.	50	No
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

**Table B–1 (Cont.) IFS.SERVICE.\* Properties**

Property	Description and Usage Note	Default	Required?
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. TraceLevelChannel <i>n</i>	Tracing verbosity for trace channel <i>n</i> . Refer to the Javadoc for class <code>oracle.ifs.common.TraceLogger</code> for a list of Oracle-defined trace levels.	none	No
IFS.SERVICE.TRACING. DefaultTraceLevel	Default tracing verbosity for all trace channels. See <code>oracle.ifs.common.TraceLogger</code> Javadoc for a list of trace levels.	none	No



---

## Server Configuration Properties

Each server has an `IFS.SERVER.Class` property that identifies the Java class that the node uses to instantiate the server or agent. You cannot change the name of the class; if you do, the protocol server or agent will not run.

The properties listed in these tables are all required for an agent or protocol server to run properly. When you install and configure an Oracle Files instance, the properties are configured using the default values shown in the tables in this section. You can change these in the base class and then create new servers or agents based on the changes, or you can change the values in the running server or agent. See [Chapter 6, "Changing Configuration Settings"](#) for additional information.

This appendix includes the following topics:

- [Access Control List Index Agent](#)
- [AppleTalk Filing Protocol \(AFP\) Server](#)
- [Content Garbage Collection Agent](#)
- [Dangling Object AV Cleanup Agent](#)
- [Distributed Authoring and Versioning \(DAV\) Server Configuration](#)
- [Event Exchanger Agent](#)
- [Expiration Agent](#)
- [File Transfer Protocol \(FTP\) Server](#)
- [Files Base Server Configuration](#)
- [Files-Specific Server Configuration](#)
- [Folder Index Analyzer Agent](#)
- [Garbage Collection Agent](#)
- [Inbound Queue Listener Agent](#)
- [Lock Agent](#)
- [NbServer \[NetBIOS\]](#)
- [Network File System \(NFS\) Protocol Server](#)
- [NT File System \(NTFS\) Protocol Server](#)
- [Print Agent](#)
- [Quota Agent](#)
- [Service Warmup Agent](#)

- [Service Watchdog Agent](#)
- [Server Message Block \(SMB\) Protocol Server](#)

## Access Control List Index Agent

The Access Control List Index Agent performs background maintenance operations on internal Oracle Files tables that are referred to collectively as the "ACL index." These tables make certain security functions (such as object discovery, ACL resolution, ACL proxies, and Workspace membership resolution) perform better.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.AccessControlListIndexAgent
```

**Table C–1 Access Control List Index Agent Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.SESSION.User</code>	User name for server session. Must be a user with Oracle Files administrator privileges.	system
<code>FS.SERVER.TIMER.InitialDelay</code>	The initial delay when the agent will first run; this allows the agents' first trigger to be staggered. h = hours, m = minutes, s = seconds	10s
<code>IFS.SERVER.TIMER.ActivationPeriod</code>	Time interval between agent activation. Default setting of 24h activates the agent every 24 hours. Set time in h (hours), m (minutes), or s (seconds).	24h
<code>IFS.SERVER.AGENT.ACCESSCONTROLLISTINDEXAGENT.MaxDeferredEntryCount</code>	Maximum number of entries to process in a single batch. The default value should rarely be modified.	10000
<code>FS.SERVER.AGENT.ACCESSCONTROLLISTINDEXAGENT.PublishStatisticsPeriod</code>	Time interval at which agent statistics are published. Set time in h (hours), m (minutes), or s (seconds).	1m

## AppleTalk Filing Protocol (AFP) Server

AppleTalk Filing Protocol (AFP) is the remote filing system protocol that enables Macintosh users to store, access, and share files over a network. AppleShare is the AFP file server that is implemented on Macintosh computers. The Oracle Files AFP server enables Macintosh users to access Oracle Files as if it were an AppleShare server.

The `IFS.SERVER.Class` that instantiates the AFP Server is:

```
oracle.ifs.protocols.afp.AfpServer
```

**Table C–2 AFP Server Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.SESSION.User</code>	User name for server session. Must be a user with Oracle Files administrator privileges.	system
<code>IFS.SERVER.PROTOCOL.AFP.AcceptGuestConnections</code>	Allows or prevents unauthenticated guest connections. Set to true to allow unauthenticated users (guests) to connect. Set to false to require authentication (thus disabling guest access).	true
<code>IFS.SERVER.PROTOCOL.AFP.DisableFolderIcons</code>	Disables or enables custom Macintosh folder icons. Set to true to disable folder icons. Set to false to enable custom folder icons. By default, custom folder icons are disabled to provide faster file browsing.	true
<code>IFS.SERVER.PROTOCOL.AFP.DisablePkgInfo</code>	Whether or not to "vanish" the special Macintosh contents/PkgInfo file. Set to true to hide all PkgInfo files. Set to false to display PkgInfo files. By default, PkgInfo files are not displayed to provide faster file browsing.	true

**Table C–2 (Cont.) AFP Server Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.PROTOCOL.AFP.Encoding</code>	The encoding to use (Java or IANA code name) to convert Macintosh strings.	MacRoman
<code>IFS.SERVER.PROTOCOL.AFP.LocalBindAddress</code>	The IP address that the server will use (bind to) when listening for incoming connections.  This value is set to the server IP address by default. It should not be modified except in unusual cases, for example, a multi-homed server.	IP address or DNS name
<code>IFS.SERVER.PROTOCOL.AFP.MaxOpenFiles</code>	Maximum number of open file forks for each connected session. Macintosh files consist of up to two forks. A connected session can open only up to this number of forks simultaneously.	1024
<code>IFS.SERVER.PROTOCOL.AFP.Port</code>	The AFP port; fixed and set to 548.	If not specified, Oracle Files uses the local host address and port 548.

## 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. This agent runs at specific times of the day as specified in the server configuration file.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.ContentGarbageCollectionAgent
```

**Table C–3 Content Garbage Collection Agent Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.AGENT.CONTENTGARBAGECOLLECTIONAGENT.FilteredContentRemovalPeriod</code>	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

## 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 directory object which was deleted and is now invalid.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.DanglingObjectAVCleanupAgent
```

**Table C–4 Dangling Object AV Cleanup Agent Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.AGENTS.DANGLINGOBJECTAVCLEANUPAGENT.ExcludedAttributeList</code>	A list of attributes for which invalid references to Library Objects 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

## Distributed Authoring and Versioning (DAV) Server Configuration

Through Web Folders (WebDAV) and Web Folders-enabled applications, you can edit Microsoft Office documents stored in Oracle Files in place with Windows Office 2000. A new document can be created in Oracle Files this way. Customers can then delete this document in a Web Folder. This servlet also serves documents over HTTP (browser).

The `IFS.SERVER.Class` that instantiates this server is:

```
oracle.ifs.protocols.dav.impl.server.IfsServletServer
```

**Table C–5 DAV Server Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.PROTOCOL.DAV.Browse.Enabled</code>	This value has no effect in Oracle Files.	N/A
<code>IFS.SERVER.PROTOCOL.DAV.ContextServletPath</code>	This value has no effect in Oracle Files.	N/A
<code>IFS.SERVER.PROTOCOL.DAV.GuestPool.Size.Max</code>	The maximum size of the anonymous session pool. This is allocated if the target size is not sufficient to service traffic volume, but will wait <code>IFS.SERVER.PROTOCOL.DAV.GuestPool.Timeout.Target</code> milliseconds before allocating.	10
<code>IFS.SERVER.PROTOCOL.DAV.GuestPool.Size.Min</code>	The minimum size of the anonymous session pool. This is allocated immediately upon startup.	1
<code>IFS.SERVER.PROTOCOL.DAV.GuestPool.Size.Target</code>	The target size of the anonymous session pool. This is allocated immediately if the target size is not sufficient to service traffic volume.	5
<code>IFS.SERVER.PROTOCOL.DAV.GuestPool.Timeout.Max</code>	The maximum time before the anonymous session pool times out. The DAV Server will wait this amount of time before returning "Server Busy" if the Max size has been reached.	1500
<code>IFS.SERVER.PROTOCOL.DAV.GuestPool.Timeout.Target</code>	The targeted time before the anonymous session pool times out. The DAV Server will wait this amount of time before allocating a new session if the Target size has been reached.	500
<code>IFS.SERVER.PROTOCOL.DAV.IfsServer.Auth.TokenCredential.Timeout</code>	When the DAV Server generates a token credential, how long should it be good for. Currently used by Oracle FileSync.  This property is measured in seconds. Set to zero to disable the token credential.	864000
<code>IFS.SERVER.PROTOCOL.DAV.Jsp.AllowedDirs</code>	This value has no effect in Oracle Files.	N/A
<code>IFS.SERVER.PROTOCOL.DAV.Jsp.Enabled</code>	Whether JSP execution is enabled. Must always be false. Do not change.	false
<code>IFS.SERVER.PROTOCOL.DAV.Jsp.Lookup.BundleName</code>	This value has no effect in Oracle Files.	N/A
<code>IFS.SERVER.PROTOCOL.DAV.Jsp.Lookup.ParameterName</code>	This value has no effect in Oracle Files.	N/A
<code>IFS.SERVER.PROTOCOL.DAV.LoginBeanName</code>	The name by which the <code>IfsHttpLogin</code> bean is bound to the <code>HttpSession</code> . Do not change.	<code>IfsHttpLogin</code>
<code>IFS.SERVER.PROTOCOL.DAV.UserLoginPool.Max</code>	How many concurrent connections a given user can have.	3
<code>IFS.SERVER.PROTOCOL.DAV.Welcome</code>	The welcome files, in the order they will be searched.	<code>index.html</code>
<code>IFS.SERVER.PROTOCOL.DAV.Webfolders.DefaultCharset</code>	This value has no effect in Oracle Files.	N/A

## Event Exchanger Agent

This agent periodically purges expired events from the event queue.



The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.EventExchangerAgent
```

**Table C–6 Event Exchanger Agent Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.EventLifespan</code>	The time, in seconds, after which an event is assumed to have been delivered and become eligible for purging.	1800

## Expiration Agent

All public objects have an attribute called `ExpirationDate`. Once 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. This agent runs at specific times of the day as specified in the server configuration parameter, `IFS.SERVER.TIMER.ACTIVATIONPERIOD`.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.ExpirationAgent
```

**Table C–7 Expiration Agent Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.SESSION.User</code>	User name for server session. Must be a user with Oracle Files administrator privileges.	system
<code>IFS.SERVER.TIMER.InitialTimeOfDay</code>	First event. Set time based on a 24 hour clock.	02:00:00
<code>IFS.SERVER.TIMER.ActivationPeriod</code>	Defines the time interval between when the agent will be triggered. h = hours, m = minutes, s = seconds.	24h

## File Transfer Protocol (FTP) Server

The FTP server allows users to easily transfer files between one file system and the Oracle Files repository. FTP is particularly useful when performing bulk transfers, in regards to both ease and performance. In addition to the common FTP commands, the Oracle Files server also has built-in parsing and versioning support.

The `IFS.SERVER.Class` that instantiates the FTP server is:

```
oracle.ifs.protocols.ftp.server.FtpServer
```

**Table C–8 FTP Server Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.PROTOCOL.FTP.Localhost</code>	Optionally, specify the host name if the host is multi-homed in the network.	Default_Hostname
<code>IFS.SERVER.PROTOCOL.FTP.AnonymousAllowed</code>	If set to true, allows anonymous connections.	true
<code>IFS.SERVER.PROTOCOL.FTP.DateFormat</code>	Specifies the default date format.	MMM dd HH:mm
<code>IFS.SERVER.PROTOCOL.FTP.Timeout</code>	Amount of time between activity before the connection times out; default is 900 seconds or 15 minutes. Unit of measure is milliseconds.	900000

**Table C–8 (Cont.) FTP Server Properties**

Property	Description and Usage Note	Default
IFS.SERVER.PROTOCOL.FTP.Delimiter	Specifies the Folder Path Delimiter.	/
IFS.SERVER.PROTOCOL.FTP.Port	The port on which the server is running.	21 (Windows), 2100 (UNIX)
IFS.SERVER.PROTOCOL.FTP.AcceptQueueSize	The number of server requests back-logged before denying requests. Do not change.	50
IFS.SERVER.PROTOCOL.FTP.AnonymousPoolSize	Initial pool size for anonymous connections.	0
IFS.SERVER.PROTOCOL.FTP.BannerText	The string that will be displayed when the FTP client is started.	Oracle Files FTP Server ready

## Files Base Server Configuration

Oracle Files uses additional server configuration properties, specific to Oracle Files. These properties are inherited and locally defined.

**Note:** If you configured Oracle Files to reuse a previously created schema, you must edit the following Files Base Server Configuration properties so that they point to the appropriate computer:

IFS.SERVER.APPLICATION.UIX.ApplicationHost

IFS.SERVER.APPLICATION.UIX.ApplicationPort

Or, you can override these properties in the server-specific configurations.

**Table C–9 Files Base Server Properties**

Property	Description and Usage Note	Default
IFS.SERVER.APPLICATION.FILES.FileSyncUrl	URL for the Oracle FileSync installation executable. Set to a relative URL if the client is on Oracle Files, or to an absolute URL if the client is on a different server.	AllPublic/Users/Users-S/system-data/downloads/FileSync.exe
IFS.SERVER.APPLICATION.FILES.PortalUrl	URL for the Back to Portal global button.	null
IFS.SERVER.APPLICATION.FILES.PrivacyStatement	Location of privacy statement relative to the folder /AllPublic/Users/Users-s/system-data/.	null
IFS.SERVER.APPLICATION.FILES.PublicBrowsingAllowed	Whether users can browse public folders without logging in. Only applies to dedicated schema mode.	true
IFS.SERVER.APPLICATION.FILES.WorkflowUrl	URL for the workflow global button.	Set during install
IFS.SERVER.APPLICATION.UIX.AdministratorEmail	The email address of the person who administers the system and receives alerts and error reports.	Set during install
IFS.SERVER.APPLICATION.UIX.ApplicationHost	The host name of the site (where a user connects; e.g., files.oracle.com).	Set during install
IFS.SERVER.APPLICATION.UIX.ApplicationPort	The port number of the site (usually 7777).	Set during install

**Table C–9 (Cont.) Files Base Server Properties**

Property	Description and Usage Note	Default
IFS.SERVER.APPLICATION.UIX.ApplicationServletMount	The mount point for the application servlet.	/files/app
IFS.SERVER.APPLICATION.UIX.ApplicationUseHttps	Whether the site uses SSL/HTTPS; e.g., https://files.oracle.com.	false
IFS.SERVER.APPLICATION.UIX.ContentServletMount	The mount point for the content/DAV servlet.	/files/content
IFS.SERVER.APPLICATION.UIX.HttpAuthManagerClass	The HTTP Authentication Manager to use. Do not change.	oracle.ifs.files.servlet.FilesHttpAuthManager
IFS.SERVER.APPLICATION.UIX.MaximumUniqueSessionsPerUser	The maximum number of distinct sessions a Web user can get. After the maximum number has been reached, the sessions are shared in a round-robin fashion.	3
IFS.SERVER.APPLICATION.UIX.OID.UserProvisioningEnabled	If set to true, enables on-demand enrollment, a process in which Oracle Files performs the necessary tasks to automatically provision a new user.	true
IFS.SERVER.APPLICATION.UIX.SSO.Enabled	If set to true, enables Single Sign-On (SSO).	true
IFS.SERVER.APPLICATION.UIX.Smtphost	The Host name of the SMTP server.	Set during install
IFS.SERVER.APPLICATION.UIX.Smtphost	The SMTP user, if the SMTP server requires a user to be specified.	Set during install
IFS.SERVER.APPLICATION.UIX.StaticResourcesMount	The mount point for the static images used to render Web pages.	/files/static

## Files-Specific Server Configuration

Oracle Files uses several server configurations that do not have properties of their own; they only inherit from other configurations. The properties of the Files-specific configurations may override properties from the inherited configurations.

**Table C–10 Files-Specific Server Configurations**

Server Configuration Name	Inherits From:
FilesAfpServerConfiguration	FilesBaseServerConfiguration, AfpServerConfiguration
FilesArchiveFileToBFileAgentConfiguration	FilesBaseServerConfiguration
FilesDelayedArchiveFileToBFileAgentConfiguration	FilesBaseServerConfiguration
FilesFtpServerConfiguration	FilesBaseServerConfiguration, FtpServerConfiguration
FilesHttpServerConfiguration	FilesBaseServerConfiguration, DavServerConfiguration
FilesNfsServerConfiguration	FilesBaseServerConfiguration, NfsServerConfiguration
FilesNtfsServerConfiguration	FilesBaseServerConfiguration, NtfsServerConfiguration
FilesOidUserSynchronizationAgentConfiguration	FilesBaseServerConfiguration
FilesReviewProcessExpirationAgentConfiguration	FilesBaseServerConfiguration
FilesSmbServerConfiguration	FilesBaseServerConfiguration, SmbServerConfiguration
FilesSubscriberExpirationAgentConfiguration	FilesBaseServerConfiguration
FilesSubscriberUsageAgentConfiguration	FilesBaseServerConfiguration

**Table C–10 (Cont.) Files-Specific Server Configurations**

Server Configuration Name	Inherits From:
FilesSubscriberUsageStatsAgent Configuration	FilesBaseServerConfiguration
FilesUserExpirationAgentConfiguration	FilesBaseServerConfiguration
FilesWorkflowLockCleanupAgent Configuration	FilesBaseServerConfiguration

### The Oracle Files HTTP Server

Do not change the name of the `FilesHttpServer`. If you change the server name, you will not be able to access Oracle Files through the Web application interface.

If you must change the `FilesHttpServer` name, you must also change the name in the `web.xml` configuration file. To change the `FilesHttpServer` name:

1. Rename the server using the Oracle Enterprise Manager Web site.
2. Edit `web.xml`, located in the following directory:

```
$ORACLE_HOME/j2ee/OC4J_iFS_files/applications/files/files/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>FilesHttpServer</param-value>
</init-param>
```

3. Save the file.
4. Restart the OC4J instance.

## Folder Index Analyzer Agent

Oracle Files 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 suboptimal state. The Folder Index Analyzer Agent runs periodically to detect and correct any such state, and return the Folder Index to an optimal state.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.FolderIndexAnalyzerAgent
```

You should never modify these values.

**Table C–11 Folder Index Analyzer Agent Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.AGENTS.FOLDERINDEXANALYZERAGENT.MaxParentsThreshold</code>	The threshold for max number of parents after which FIS is considered suboptimal. This condition is ANDed with the <code>MaxChildrenThreshold</code> .	10
<code>IFS.SERVER.AGENTS.FOLDERINDEXANALYZERAGENT.MaxChildrenThreshold</code>	The threshold for max number of children after which FIS is considered suboptimal. This condition is ANDed with the <code>MaxParentsThreshold</code> .	10

## Garbage Collection Agent

The Garbage Collection Agent runs at specific times of the day as specified in the server configuration file. Currently, this agent fixes invalid Public Object owners, creators, deletors, and modifiers.

For example, a document is created and modified by "jsmith." The creator, owner, and last modifier attribute of document are set to jsmith's object ID. If "jsmith" is deleted, the attribute value becomes invalid. The agent replaces these invalid attribute values with the ID of the replacement owner, creator, or deleter specified in the server configuration file.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.GarbageCollectionAgent
```

**Table C–12 Garbage Collection Agent Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementOwner</code>	User to be replaced as owner. Modify as needed.	system
<code>IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementDeletor</code>	User to be replaced as deleter. Modify as needed.	system
<code>IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementCreator</code>	User to be replaced as creator. Modify as needed.	system
<code>IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementModifier</code>	User to be replaced as modifier. Modify as needed.	system

## 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 Files 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 `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.InboundQueueListenerAgent
```

**Table C–13 Inbound Queue Listener Agent Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.AGENT.INBOUNDQUEUELISTENERAGENT.Queues</code>	Holds a list of queues that the agent will listen on.	IFS_IN

## Lock Agent

The Lock Agent is a time-based agent that releases locks that are timed out. The agent needs to be running at all times for the lock auto-expiration function to work.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.LockAgent
```

## NbServer [NetBIOS]

The NbServer is a name server for Windows NetBIOS names. It tells client computers that its name is registered to a particular IP address.

The `IFS.SERVER.Class` that instantiates this server is:

```
oracle.ifs.protocols.smb.server.NbServer
```

**Table C–14 Nb Server Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.NB.Workgroup</code>	Name of the workgroup this server is in.	WORKGROUP
<code>IFS.SERVER.NB.ServerComment</code>	This holds the SMB server description that shows up in properties in Windows.	Oracle Internet File Server
<code>IFS.SERVER.NB.IpAddr</code>	If host is multi-homed, use this to choose the IP address if necessary	IP Address returned by <code>Socket.getInetAddress()</code>
<code>IFS.SERVER.NB.Netmask</code>	NetMask for the name server. This is used to derive the broadcast address. No need to set this if the broadcast address is specified explicitly.	255.255.252.0
<code>IFS.SERVER.NB.Broadcast</code>	Broadcast address. Use this if you know the broadcast address or want to override the address derived from the netmask. This is specified as a standard IP string (for example, 144.25.103.255).	Derived from the IP address and netmask
<code>IFS.SERVER.NB.StatusInterval</code>	Number of packets between each status message to trace file.	100
<code>IFS.SERVER.NB.HostAnnouncer</code>	Enables Host Announcement.	true

## Network File System (NFS) Protocol Server

The Network File System (NFS) protocol is used to provide file sharing between a client computer and a server computer across a network. The NFS protocol is a standard protocol which is widely used for file sharing on UNIX platforms. Although used primarily on UNIX platforms, the NFS protocol is designed to be operating system-independent and implementations of the NFS protocol exist for other platforms, such as Windows.

See ["Using Oracle Files with NFS"](#) on page 2-8 for information about configuring the NFS server, including mapping UNIX UIDs to Oracle Files user accounts, setting up a trusted client list, and enabling NIS authentication.

The `IFS.SERVER.Class` that instantiates the NFS server is:

```
oracle.ifs.protocols.nfs.server.NfsServer
```

**Table C–15 NFS Server Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.PROTOCOL.NFS.Localhost</code>	Specifies the IP address the server will listen on if the server computer is capable of listening on multiple IP addresses. This is the same as the Localhost parameter on other protocol servers.	null
<code>IFS.SERVER.PROTOCOL.NFS.PortmapUdpServers</code>	Specifies the number of UDP server threads to be started for the Portmap server. The number of UDP server threads determines how many simultaneous UDP requests the Portmap server can handle.	1
<code>IFS.SERVER.PROTOCOL.NFS.PortmapTcpEnabled</code>	Specifies whether or not the Portmap server will accept TCP connections in addition to UDP connections.	true
<code>IFS.SERVER.PROTOCOL.NFS.MountUdpServers</code>	Specifies the number of UDP server threads to be started for the Mount server. The number of UDP server threads determines how many simultaneous UDP requests the Mount server can handle.	1

**Table C–15 (Cont.) NFS Server Properties**

Property	Description and Usage Note	Default
IFS.SERVER.PROTOCOL.NFS.MountTcpEnabled	Specifies whether or not the Mount server will accept TCP connections in addition to UDP connections.	true
IFS.SERVER.PROTOCOL.NFS.MountPort	Specifies the port number which the Mount server will listen on. A value of zero will use any available port.  The Mount server will normally use any available port number and then register the port number being used with the Portmap server. A specific port number should be specified if the Mount server is a secondary server and does not register the port with the Portmap server.	4048 for UNIX; 0 for Windows platforms
IFS.SERVER.PROTOCOL.NFS.UdpServers	Specifies the number of UDP server threads to be started for the NFS server.  The number of UDP server threads determines how many simultaneous UDP requests the NFS server can handle.	16
IFS.SERVER.PROTOCOL.NFS.TcpEnabled	Specifies whether or not the NFS server will accept TCP connections in addition to UDP connections.	true
IFS.SERVER.PROTOCOL.NFS.Port	Specifies the port number which the NFS server will listen on.  The standard port number for the NFS server is port 2049. On UNIX systems, the standard UNIX NFS server will be running on the standard port, therefore the Oracle Files NFS server is configured to be a secondary NFS server running on a different port number.	4049 for UNIX; 2049 for Windows platforms
IFS.SERVER.PROTOCOL.NFS.TrustedClientsEnabled	Enable Trusted Client List feature.	false
IFS.SERVER.PROTOCOL.NFS.TrustedClientList	List of trusted NFS clients.	<"">
IFS.SERVER.PROTOCOL.NFS.NISEnabled	Used to indicate if NIS is used for user management.	false
IFS.SERVER.PROTOCOL.NFS.NISServiceProvider	Provider of NIS service. This is an NIS server.	<"">
IFS.SERVER.PROTOCOL.NFS.CharacterEncoding	Specifies the character encoding to be used to interpret string such as file names that the NFS server receives from the clients. The value is the name of a Java character encoding. For example: ASCII, ISO8859_1, or Cp437. A null value indicates that the default character encoding should be used.	null
IFS.SERVER.PROTOCOL.NFS.UserCacheMax	Specifies the number of Oracle Files user sessions the NFS server will keep open.  This value should be set to the expected number of simultaneous active users.	16
IFS.SERVER.PROTOCOL.NFS.AllowAnonymousUser	Allows users to login as anonymous/guest.	true
IFS.SERVER.PROTOCOL.NFS.ResetUserCache	Used to control the resetting of the user cache. Used when privileges are changed.	0
IFS.SERVER.PROTOCOL.NFS.IoBufferSize	Specifies the I/O buffer size. The I/O buffer size determines the largest amount of data that can be read or written in a single request to the NFS server.	32768
IFS.SERVER.PROTOCOL.NFS.IoBufferCacheTargetSize	Specifies the number of I/O buffers that the NFS server will try to allocate.  This should be set to the expected number of simultaneous I/O operations.	8
IFS.SERVER.PROTOCOL.NFS.ContentCacheFlush	Specifies the write flush time-out value in milliseconds. The default value of 2000 means that writes to an Oracle Files document will be committed to the database after 2 seconds.  Setting too low of a time-out value may cause additional database commits resulting in slower performance. Setting too high a time-out value will cause a delay before the data is committed and is available to other protocols.	2000

**Table C–15 (Cont.) NFS Server Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.PROTOCOL.NFS.ContentCacheKeep</code>	Specifies the keep time-out value in milliseconds. The default value of 10000 means that once a document is opened, the NFS server will attempt to cache its contents for 10 seconds.	10000
<code>IFS.SERVER.PROTOCOL.NFS.ContentCacheMax</code>	Specifies the maximum number of documents the NFS server will keep in its content cache.  Increasing the content cache size improves performance but will use additional database connections.	8
<code>IFS.SERVER.PROTOCOL.NFS.RpcRequestCacheBufferSize</code>	Specifies the size of the request cache buffer. The request cache maintains a history of recent requests and is used to return a reply when a duplicate request is received from a client.	65535
<code>IFS.SERVER.PROTOCOL.NFS.RpcRequestCacheMax</code>	Specifies the maximum number of requests to be kept in the request cache. The request cache maintains a history of recent requests and is used to return a reply when a duplicate request is received from a client.	64
<code>IFS.SERVER.PROTOCOL.NFS.RpcRequestCacheMaxReplyLen</code>	Specifies the maximum length of a reply to be kept in the request cache. The request cache maintains a history of recent requests and is used to return a reply when a duplicate request is received from a client.	16384
<code>IFS.SERVER.PROTOCOL.NFS.SafeWriteMode</code>	Specifies whether or not SafeWriteMode is enabled. If true, data written to NFS will be logged to the local disk in addition to being written to the database.	false
<code>IFS.SERVER.PROTOCOL.NFS.SafeWriteLogs</code>	Specifies the directory where the recovery log files will be written if SafeWriteMode is enabled.  The path specified is relative to the Oracle Files home directory where Oracle Files was installed.	nfs/Recovery Logs
<code>IFS.SERVER.PROTOCOL.NFS.SafeWriteActivationPeriod</code>	Specifies the activation period for the SafeWriteMode recovery thread in minutes. The default value of 20 indicates that the SafeWriteMode recovery thread will run every 20 minutes.	20

## NT File System (NTFS) Protocol Server

For Windows platforms only.

The NT File System (NTFS) allows the Oracle Files repository to appear as a local hard drive on the server computer. When using NTFS, the Oracle Files repository will be mapped to a drive letter on the server computer and can be accessed using the file system as if it were a local hard drive.

The `IFS.SERVER.Class` that instantiates the NTFS server is:

```
oracle.ifs.protocols.ntfs.server.NtfsServer
```

**Table C–16 NTFS Server Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.PROTOCOL.NTFS.DriveLetter</code>	The drive letter used to map the Oracle Files drive.  An available and valid drive letter (A - Z).	O
<code>IFS.SERVER.PROTOCOL.NTFS.LogLevel</code>	Specifies the type of information listed in the log file.  A number from 1 to 4. 1 is the minimum and 4 is the maximum information in the log file.	1



**Table C–16 (Cont.) NTFS Server Properties**

Property	Description and Usage Note	Default
<code>IFS.SERVER.PROTOCOL.NTFS.LogStackTrace</code>	Specifies if the Java stack trace is listed in the log file. true = list Java stack trace. false = do not list Java stack trace.	false
<code>IFS.SERVER.PROTOCOL.NTFS.SessionCache</code>	Specifies the number of user sessions the NTFS server will keep open. This value should be set to the expected number of simultaneously opened files.	40
<code>IFS.SERVER.PROTOCOL.NTFS.ifsproxy</code>	Specifies the location of the <code>ifsproxy.dll</code> library. The path specified is relative to the Oracle Files home directory where Oracle Files was installed.	<code>lib/ifsproxy.dll</code>

## Print Agent

The Print Agent makes printing through Oracle Files indistinguishable from printing to a normal Windows server.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.print.PrintAgent
```

## Quota Agent

The Quota Agent is triggered by an event to compute the consumed quota for users or Workspaces. This agent also periodically checks all users who are active, according to a specified timer period. The agent updates the user's consumed storage. When the consumed storage is over the allocated quota, the user will not be able to add any more documents to Oracle Files.

A user's quota is calculated upon the content already consumed. Therefore, a user will go over quota by adding the final file that pushes the consumed storage over the allocated storage. When setting users' allocated quota, remember that a user's last file will put him or her over quota before being denied.

Quotas will not be enforced if:

- The Quota Agent has not been started or is not running.
- The user's quota has not been enabled.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.QuotaAgent
```

## Service Warmup Agent

When a node is started, this agent automatically preloads the service's data cache. It expects the following entries in the Server Configuration file.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.ServiceWarmupAgent
```

**Table C-17 Service Warmup Agent Properties**

Property	Description and Usage Note	Default
IFS.SERVER.AGENT.SERVICEWARMUP.WarmupSetAdmin	If the preloading is done in administration mode.	true
IFS.SERVER.AGENT.SERVICEWARMUP.WarmupUsers	If set to true, preloads user collection.	false
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

## Service Watchdog Agent

The Service Watchdog Agent cleans up after Oracle Files services that do not shut down cleanly.

The `IFS.SERVER.Class` that instantiates this agent is:

```
oracle.ifs.management.servers.ServiceWatchdogAgent
```

**Table C-18 Service Watchdog Agent Properties**

Property	Description and Usage Note	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

## Server Message Block (SMB) Protocol Server

The SMB server allows Windows clients to easily copy files between their local drives and the Oracle Files repository. It also allows users to browse and edit files and even execute programs directly from the Oracle Files repository. SMB is best suited for interactive browsing and modifying documents.

You should configure the `NbServer` for use with SMB; see "[NbServer \[NetBIOS\]](#)" on page C-9 for more information.

The `IFS.SERVER.Class` that instantiates this server is:

```
oracle.ifs.protocols.smb.server.SmbServer
```

**Table C-19 SMB Server Properties**

Property	Description and Usage Note	Default
IFS.SERVER.PROTOCOL.SMB.ServerComment	Holds the SMB server description that shows up in the Windows Properties window.	Oracle Internet File Server
IFS.SERVER.PROTOCOL.SMB.PrimeServer	Primes the server with a simple login.	true
IFS.SERVER.PROTOCOL.SMB.EnablePrinting	If set to true, allows users to print through the SMB Server to configured printers. You cannot use Oracle Files printing services without this property enabled.	true
IFS.SERVER.PROTOCOL.SMB.EnableOplocks	If this parameter is true, it lets client cache their reads and writes and results in improved performance.  If set to true, this may cause problems with consistency across all the protocols; however, true yields better performance.	true

**Table C-19 (Cont.) SMB Server Properties**

Property	Description and Usage Note	Default
IFS.SERVER.PROTOCOL.SMB.MaxOplocks	Maximum number of Op Locks per mount point. See Microsoft documentation for information about Op Locks.	8
IFS.SERVER.PROTOCOL.SMB.KeepStats	If true, keeps statistics on various server operations.	true
IFS.SERVER.PROTOCOL.SMB.PrintStats	If true, prints statistics on SMB commands into the log file after the user disconnects.	Defaults to true if the log level for the node is medium or greater.
IFS.SERVER.PROTOCOL.SMB.ShareMyHome	Specifies if the virtual MyHome mount point is shared as a mount point.  true = include MyHome in the list of mount points false = do not include MyHome in the list of mount points	true
IFS.SERVERPROTOCOL.SMB.Workgroup	Windows workgroup.  This determines the workgroup where the SMB server will appear in the Network Neighborhood.	WORKGROUP
IFS.SERVER.PROTOCOL.SMB.Port	Port for the SMB server to listen on.  All Windows clients require the SMB server to listen on the default port, 139. Only processes with root privileges can listen on low-numbered ports, so the SMB server must be run as root.	139
IFS.SERVER.PROTOCOL.SMB.AllowGuestIfNotUser	Allows users who do not have valid accounts on this server to browse as a guest.  true = allows non-guest users as guest. false = forces a valid username.	true
IFS.SERVER.PROTOCOL.SMB.MaxOpenFiles	The maximum number of files a user can have open on a single mountpoint.	30
IFS.SERVER.PROTOCOL.SMB.MaxAllOpenFiles	The total number of open files the SMB server allows across all users.  The total is also limited by the number of connections configured for the SMB server and database.	100
IFS.SERVER.PROTOCOL.SMB.SessionTimeout	The server will disconnect idle sessions after this timeout.  Unit of measure is in milliseconds.	43200000 (12 hours)
IFS.SERVER.PROTOCOL.SMB.IpAddress	The IP address that is advertised as the location for the SMB server.  This value is defaulted from the server IP address and should not be modified except in unusual cases, for example, multi-server.	server IP address
IFS.SERVER.PROTOCOL.SMB.HostName	Name of the SMB server.	The computer name where the server is running.
IFS.SERVER.PROTOCOL.SMB.ForceLowerCase	Forces lowercase filenames.	false



---

## Setting Up Oracle Files With RAC

This appendix describes how to configure Oracle Files to leverage the features of Oracle9i Real Application Clusters (RAC). It provides high-level background information about RAC and discusses the configuration steps that must be performed to allow Oracle Files to function properly with a RAC configuration.

This appendix includes the following topics:

- [About Oracle9i Real Application Clusters](#)
- [Oracle Files Load Balancing and Failover in a RAC Environment](#)
- [Oracle Files Configuration Tasks for RAC](#)

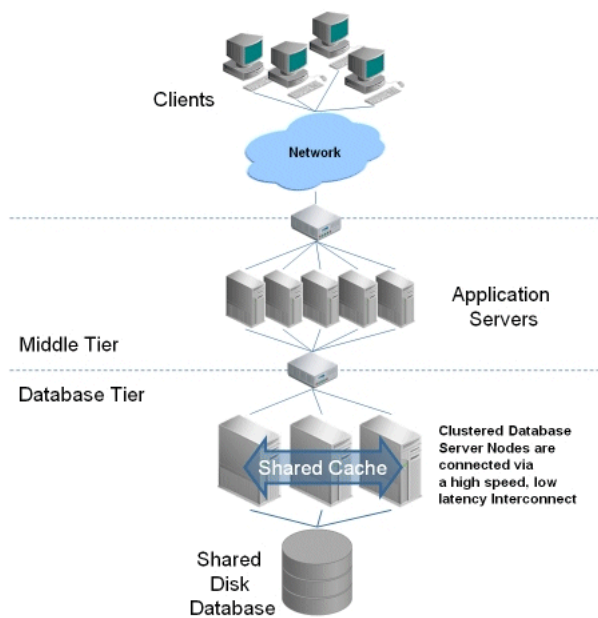
### About Oracle9i Real Application Clusters

A cluster is a group of computers acting together that behave like a single system. Clustering requires both hardware (interconnect) and software (clusterware) support. Traditionally, clusters were used in high availability read-only applications, such as data warehouses. These days, clusters are increasingly becoming a lower-cost approach to computing applications that require very high availability and scalability.

An Oracle9i Real Application Cluster consists of 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.

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 greatly simplify the installation and administration of Oracle9i Real Application Clusters.

See [Figure D-1](#) for an example of a RAC configuration.

**Figure D–1 Sample RAC Configuration**

For more information about Oracle9i RAC, see *Oracle9i Real Application Clusters Concepts*.

## Oracle Files Load Balancing and Failover in a RAC Environment

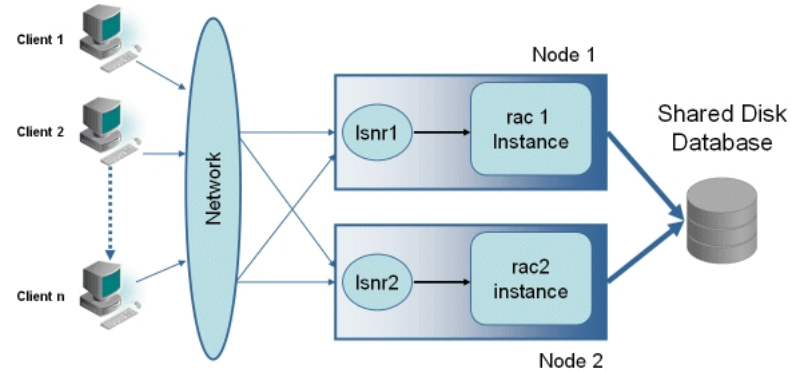
The following sections provide information on load balancing, failover, and connect descriptor settings:

- [Client Load Balancing](#)
- [Listener Load Balancing](#)
- [Recommended Load Balancing Configuration](#)
- [Oracle Files Connect Descriptor Settings for RAC](#)

### Client Load Balancing

Oracle9i RAC is a set of instances operating against the same database. The instances have a common service name, but distinct instance names. In order to enable client load balancing, you should set up multiple database listeners. Clients can balance connection requests across these listeners by supplying a list of listener addresses in their connect descriptor, which Net8 will use on a round-robin basis.

[Figure D–2](#) illustrates client load balancing.

**Figure D–2 Client Load Balancing****Example D–1 Sample tnsnames.ora Entry Enabling Load Balancing**

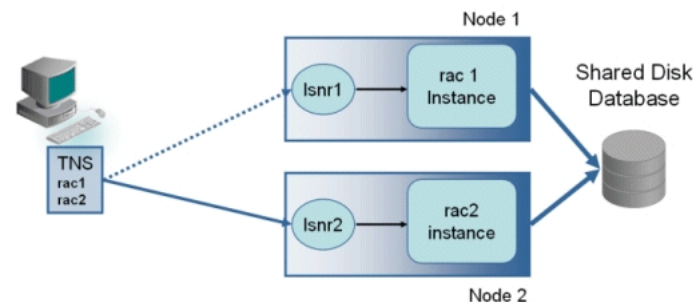
```

myrac.us.oracle.com =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = myrac1.us.oracle.com) (PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP) (HOST = myrac2.us.oracle.com) (PORT = 1521))
    (LOAD_BALANCE = ON)
    (FAILOVER = OFF)
    (CONNECT_DATA =
      (SERVICE_NAME = myrc.us.oracle.com)
      (FAILOVER_MODE = (TYPE=SELECT) (METHOD=BASIC))
    )
  )

```

### Connect Time Failover

Another benefit of multiple listeners is fault-tolerance of listener failure. Clients can failover to alternate listeners at connect time by supplying a list of listeners in their connect descriptor. [Figure D–3](#) illustrates connect time failover.

**Figure D–3 When lsnr1 Fails, Requests Can Be Re-routed to lsnr2****Example D–2 Sample tnsnames.ora Entry Enabling Failover**

```

myrac.us.oracle.com =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = myrac1.us.oracle.com) (PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP) (HOST = myrac2.us.oracle.com) (PORT = 1521))
  )

```

```
(LOAD_BALANCE = OFF)
(FAILOVER = ON)
(CONNECT_DATA =
  (SERVICE_NAME = myrc.us.oracle.com)
  (FAILOVER_MODE = (TYPE=SELECT) (METHOD=BASIC))
)
```

### Transparent Application Failover

Transparent Application Failover (TAF) allows an existing connection to fail over to another listener, without needing to reestablish the connection. The in-progress transaction must be rolled back, but there is no need to reestablish the database connection. Cursors may be optionally preserved (with a performance overhead for all normal select operations). Clients request TAF through the connect descriptor.

By setting the `<DatabaseUrl>` entry in the `registry.xml` configuration file, Oracle Files services can opt-out of the default connect descriptor and specify a connect identifier whose corresponding connect descriptor specifies the `FAILOVER_MODE` and failover listeners.

---

---

**Note:** Network protocol timeout parameters between the middle tier application and the database tier may affect the failover operation, since their values will determine the length of time that is waited before switching over to another node. It is important to ensure that these are set to an appropriately short time. On some systems, the default values for the `tcp_ip_abort_interval` and the `tcp_keepalive_interval` are set to several minutes; keeping these defaults could increase the time it takes for the system to fail over if a server node fails.

---

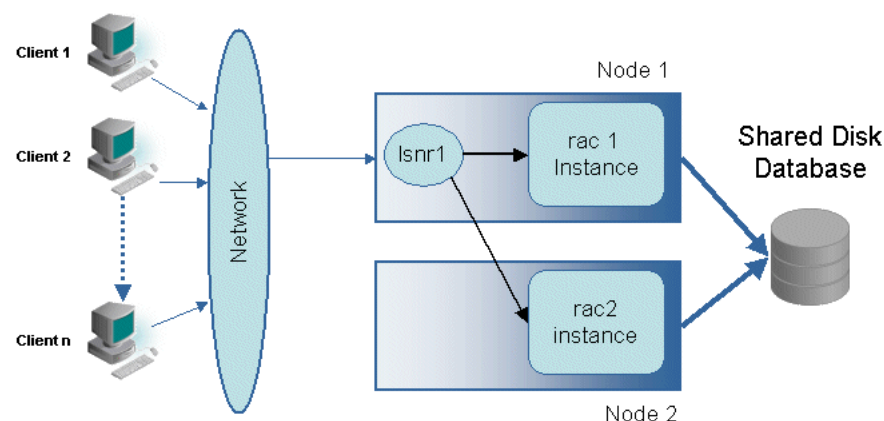
---

## Listener Load Balancing

A database listener sitting in front of multiple RAC instances can provide load balancing across them. The listener is aware of each instance, whether it is running or down, and its load. In creating a database connection, a client generally specifies only the database service name and listener address, and not the instance name, in order to defer instance selection to the listener's load balancing algorithm. This is called listener or connection load balancing (see [Figure D-4](#)).

For more information about listeners and database connections, see the *Oracle9i Net Services Administrator's Guide*.



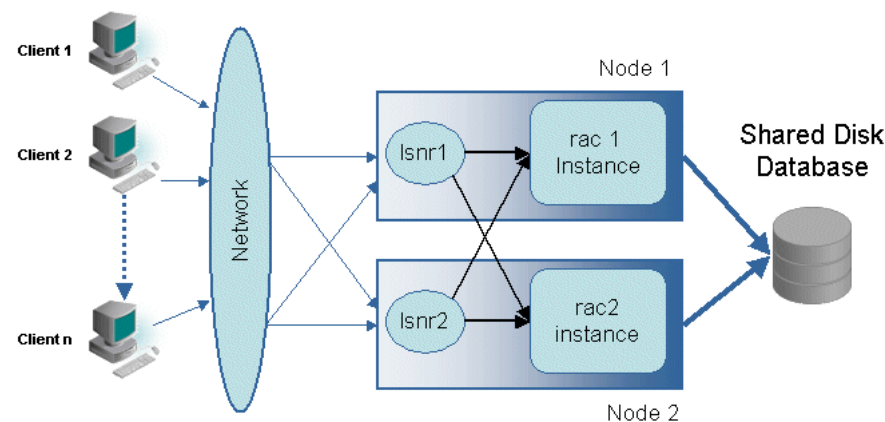
**Figure D-4 Listener Load Balancing**

If you configure your system for listener-only load balancing, note the following:

- You do not need to set the `<DatabaseUrl>` property in `registry.xml`. For more information, see ["Oracle Files Connect Descriptor Settings for RAC"](#) on page D-5.
- You cannot use TAF.
- The listener becomes a single point of failure for your system.

## Recommended Load Balancing Configuration

For optimal high availability and performance, you should configure your system for both client and listener load balancing. [Figure D-5](#) illustrates this scenario.

**Figure D-5 Client and Listener Load Balancing**

## Oracle Files Connect Descriptor Settings for RAC

When planning to use Oracle Files in a RAC environment, you should set the `<DatabaseUrl>` property in `registry.xml` since this value can be used by the Domain Controller, the management and administration tools, and the Oracle Files nodes during their operation. You must set this entry on all middle tiers.

If you are setting up your system for listener-only load balancing, you do not need to set the `<DatabaseUrl>` property in `registry.xml`. Oracle Files will synthesize a minimally-defined connect descriptor from the domain name.

## Oracle Files Configuration Tasks for RAC

Read the following sections for information on preconfiguration, configuration, and post-configuration tasks for Oracle Files in a RAC environment.

### Preconfiguration Tasks

You can choose to run Oracle Files against a Oracle9i Real Applications Clusters database at any time, either preconfiguration or post-configuration. However, if you know that you want to point to a RAC database for your initial Oracle Files deployment, perform the preconfiguration steps listed in the following sections.

#### Setting MAX\_COMMIT\_PROPAGATION\_DELAY

You should set the MAX\_COMMIT\_PROPAGATION\_DELAY system parameter in the RAC database as follows:

```
MAX_COMMIT_PROPAGATION_DELAY=1
```

During Oracle Files configuration and operation, objects are often created and then read back right away for various reasons, like the creation of subclasses or keeping middle-tier caches up-to-date. In a RAC configuration, looking for a data value from instance A that was committed by instance B can cause problems if instance A does not yet have the updated information. For this reason, you should set the MAX\_COMMIT\_PROPAGATION\_DELAY to a very small value so that the information is instantaneously made available to all instances.

Setting MAX\_COMMIT\_PROPAGATION\_DELAY to zero or to any value below 100 will have the same effect, that is to use the broadcast on commit System Change Number (SCN) generation scheme. By default, the system uses a scheme called the Lamport scheme and a MAX\_COMMIT\_PROPAGATION\_DELAY value of 700 hundredths of a second, or seven seconds. You can see this in the alert .log file ("Picked xxx scheme to generate SCNs"). The only exception is Tru-64: on that platform, setting MAX\_COMMIT\_PROPAGATION\_DELAY to zero is not recommended because it causes excessive system CPU consumption. Unfortunately, zero is the default on Tru-64, so this value must be changed for this platform. Setting the parameter to anything between 1 and 99 will have the desired broadcast on commit behavior, although it will not be reported as such in the alert .log file (instead it will say "Picked Lamport Server scheme to generate SCNs"). The bottom line is that if you want to set this parameter to a value that guarantees broadcast on commit for all platforms, select a value between 1 and 99. The fact that the parameter is a number in hundredths of a second is misleading, as anything between 1 and 99 works exactly the same way.

#### Setting JOB\_QUEUE\_PROCESSES

Ensure that the JOB\_QUEUE\_PROCESSES parameter is set to a value of 10 or higher. This parameter is required for running Oracle Files database jobs and is typically not set high enough (it may even be 0 by default).

#### Creating a TNS Entry in tnsnames.ora

Make a TNS entry in the tnsnames.ora file for load balancing and connection failover options in each Oracle home used by Oracle Files. See *Oracle9i Real Application Clusters Administration* for more information on making a TNS entry for these options. Here is a sample TNS entry which specifies multiple hosts for use in a RAC environment using sample address values:

```
myrac.us.oracle.com =  
  (DESCRIPTION =
```

```

(ENABLE = BROKEN)
(ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP) (HOST = myrac1.us.oracle.com) (PORT = 1521))
  (ADDRESS = (PROTOCOL = TCP) (HOST = myrac2.us.oracle.com) (PORT = 1521))
)
(LOAD_BALANCE = ON)
(FAILOVER = ON)
(CONNECT_DATA =
  (SERVICE_NAME = myrc.us.oracle.com)
  (FAILOVER_MODE=(TYPE=select) (METHOD=basic) (RETRIES=20) (DELAY=15))
)
)

```

For general information about TNS entries, see the *Oracle9i Net Services Reference Guide*.

## Configuration Tasks

Configure Oracle Files, specifying the name of the RAC database on the Database Selection screen of the Oracle Files Configuration Assistant.

---

**Important:** In order to use RAC, you must configure Oracle Files against a specific node in the target RAC configuration, and this node must have load balancing disabled during the Oracle Files configuration process.

---

For information about how to configure Oracle Files using the Oracle Files Configuration Assistant, see the *Oracle Collaboration Suite Installation and Configuration Guide*.

## Post-Configuration Tasks

Perform the post-configuration tasks listed in the following sections if you are using Oracle Files with a RAC database.

### Adding a <DatabaseUrl> Entry to registry.xml

On each middle tier, back up and then edit the `registry.xml` file (located in `$ORACLE_HOME/ifs/common/`) to add a <DatabaseUrl> entry. You can add the <DatabaseUrl> entry anywhere between <Instance> and </Instance>.

In the following example, the entry is added directly under the tag. Note that the TNS value you specify should be the same as that specified in the RAC pre-configuration steps.

```

<Instance>
  <DatabaseUrl>jdbc:oracle:oci8@myrac.us.oracle.com</DatabaseUrl>
  <Domain>ifs://DBHOME:1521:dbservice:ifssys</Domain>
  <DomainType>files</DomainType>
  <Registered>1018925008096</Registered>
  <LastModified>1028330926700</LastModified>
  <LastStarted>1028329087966</LastStarted>
  <Ports></Ports>
</Instance>

```

### RAC Settings for Grid Control

If you are using the Oracle Enterprise Manager Grid Control, you need to configure the Oracle Files target in the Grid Control for a RAC environment.

The Grid Control provides Oracle Files SQL metrics, such as Document Statistics, Documents By MIME Type, and Users. For these metrics to work against a RAC database, you must properly configure the `DBConnectDescriptor` for the Oracle Files target in the Grid Control.

The value of `DBConnectDescriptor` can be either a naming service connect identifier in the `tnsnames.ora`, or an explicit identifier for the database connect descriptor. If you choose to specify a naming service connect identifier, you must create a TNS entry in the `tnsnames.ora` file that resides in the Oracle home of the Grid Control Management Agent that resides on the Oracle Files middle tier.

For details on how to set this property, see *Oracle Enterprise Manager Managing Oracle Collaboration Suite* on the Oracle Technology Network at:

<http://otn.oracle.com>

---

# Migrating Data to Oracle Files

This appendix tells you how to migrate content and users from legacy systems to Oracle Files. Topics include:

- [Migrating Data from Other File Servers](#)

## Migrating Data from Other File Servers

Oracle Files does not currently offer a migration toolkit. You must migrate your files manually. The following sections provide suggestions on how to accomplish this task.

### Server Consolidation Checklist

Consolidating users, folder hierarchy, content, and access privileges from other file server systems to Oracle Files involves the following steps:

- [Migrating Users](#). You need to move the user list from the old system to the new one. In other words, you need to recreate each user in Oracle Files (by creating users in Oracle Internet Directory).
- [Creating Workspaces](#). If your old file system has user groups, you can create corresponding Workspaces in Oracle Files with the same membership.
- [Migrating Content](#). You must copy the actual files and folders from the old system to the new one.

### Migrating Users

The first task in moving to a new Oracle Files server is creating the user list. For each user you want to migrate to Oracle Files, you must create a new user in Oracle Internet Directory. For detailed information on this process, see the *Oracle Internet Directory Administrator's Guide*.

### Creating Workspaces

In order to migrate user groups from your old file system, you must create corresponding Workspaces in Oracle Files, then add the appropriate users to them.

#### Scripted Workspace 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 Workspace Creation tool to create corresponding workspaces in Oracle Files.

See ["Bulk Administration Tools for Oracle Files"](#) on page 4-6 for more information about the Workspace Creation tool.

## Migrating Content

After creating users and Workspaces, the next step is to move files and folders into Oracle Files.

Some information cannot be retained:

- **Last Modified Date.** The date and time you copy the file into Oracle Files will be the Last Modified Date.
- **Creator/Owner.** The administrator performing the migration will be listed as the file's creator.
- **Application-Specific Metadata.** If your old file system had application-specific metadata, this information cannot be automatically copied across.

### Protocols for Copying Data

Use one of the following network protocols to copy your files:

- **FTP:** The most lightweight protocol, FTP will move large amounts of data faster than the other protocols. For bulk operations, such as migrating from an existing system, FTP is the protocol of choice. You need to use either command line FTP or a GUI FTP client for this step. See [Appendix F, "FTP Quote Command Reference"](#) for more information about the FTP Quote commands.

To FTP your files into Oracle Files, the following requirements must be met:

- An FTP client must be installed on your local computer.
- You must know the port number for FTP, which was specified during Oracle Files configuration. Use the Oracle Enterprise Manager Web site to check the `IFS.SERVER.PROTOCOL.FTP.Port` property if you are unsure.
- An account on the Oracle Files server must be already set up.

To FTP your files into Oracle Files:

1. Using an FTP client, log into the Oracle Files server. You can use either the hostname of the Oracle Files server or its IP address.
2. Navigate to the files on your local computer that you want to load into Oracle Files and use your FTP client's utilities to load the files.

By default, FTP requires an Oracle Files-specific password in order to be used. You can set this password in the User Preferences page in Oracle Files; see the Oracle Files online help for more information.

- **WebDAV (Web Folders):** WebDAV, a protocol designed for Internet and intranet collaboration on files, allows you to drag and drop data from one system to another.

In order to enable WebDAV access, go to the Protocol Access page in Oracle Files and enter your SSO password. See the Oracle Files online help for more information.

In Windows:

1. Connect to a Web Folder.
2. Select the files from your local directory.

3. Drag and drop the files into a folder on the Oracle Files drive.

If you want to retain the file structure, click and drag the entire directory structure from the original file system into Oracle Files, or drag different parts of the directory tree separately, confirming that each part of the tree has been copied before copying the next one.

4. Log into Oracle Files through Windows as a test user and verify that all the files and folders are accessible.

- **SMB/NTFS:** The Windows file-sharing protocol SMB (called NTFS when the Oracle Files server is running on Windows) also provides the ease of drag-and-drop copy operations from one system to another. SMB is a more complex protocol than FTP and requires some sacrifice of performance for ease of use.

In order to enable SMB access, go to the Protocol Access page in Oracle Files and enter your SSO password. See the Oracle Files online help for more information.

- **NFS:** The Network File System (NFS) protocol is used to provide file sharing between a client computer and a server computer across a network. The NFS protocol is a standard protocol which is widely used for file sharing on UNIX platforms.





---

## FTP Quote Command Reference

This appendix provides information on using the FTP quote commands.

Topics include:

- [CASCADEOFF](#)
- [CASCADEON](#)
- [DELIM](#)
- [SETLANGUAGE](#)
- [SETCHARENCODING](#)
- [SHOWCHARENCODING](#)
- [SHOWLANGUAGE](#)

### CASCADEOFF

When deleting a folder (`rmdir`), turns off cascade delete for the session. Only empty folders will be deleted by the `rmdir` command. If folders under the directory are not empty, the `rmdir` will not succeed.

Syntax	Example
<code>quote cascadeoff</code>	<code>quote cascadeoff</code>

### CASCADEON

When deleting a folder (`rmdir`), turns on cascade delete for the session so that the folder and all its contents, including any non-empty folders, are deleted. The example shows that any folder and its contents will be deleted.

Syntax	Example
<code>quote cascadeon</code>	<code>quote cascadeon</code>

### DELIM

Sets the folder path delimiter for the current session. The example sets the character "\" to delimit folder paths.

Syntax	Example
<code>quote delim [character]</code>	<code>quote delim \</code>

## 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 the *Oracle9i Database Globalization Support Guide*.

Syntax	Example
<code>quote setlanguage [language]</code>	<code>quote setlanguage French</code> <code>quote setlanguage "Latin American Spanish"</code>

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	Egyptian	Japanese	Russian
Arabic	English	Korean	Simplified Chinese
Bengali	Estonian	Latin American Spanish	Slovak
Brazilian Portuguese	Finnish	Latvian	Slovenian
Bulgarian	French	Lithuanian	Spanish
Canadian French	German	Malay	Swedish
Catalan	Greek	Mexican Spanish	Thai
Croatian	Hebrew	Norwegian	Traditional Chinese
Czech	Hungarian	Polish	Turkish
Danish	Indonesian	Portuguese	Ukrainian
Dutch	Italian	Romanian	Vietnamese

## SETCHARENCODING

Sets the character encoding to an IANA character set name for the session when loading documents. Should be used 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 on character encodings, see the *Oracle9i Database Globalization Support Guide*.

Syntax	Example
<code>quote setcharencoding [character encoding]</code>	<code>quote setcharencoding UTF-8</code>

Valid character encodings include:

BIG5	ISO-2022-KR	KOI8-R	WINDOWS-1252
EUC-JP	ISO-8859-1	KS_C_5601-1987	WINDOWS-1253
EUC-TW	ISO-8859-2	SHIFT_JIS	WINDOWS-1254
GB2312	ISO-8859-3	TIS-620	WINDOWS-1255
IBM850	ISO-8859-4	UTF-8	WINDOWS-1256
IBM852	ISO-8859-5	WINDOWS-936	WINDOWS-1257
IBM857	ISO-8859-6	WINDOWS-949	WINDOWS-1258
IBM866	ISO-8859-7	WINDOWS-950	
ISO-2022-CN	ISO-8859-8	WINDOWS-1250	
ISO-2022-JP	ISO-8859-9	WINDOWS-1251	

## SHOWCHARENCODING

Displays the current character encoding setting for the session.

Syntax	Example
<code>quote showcharencoding</code>	<code>quote showcharencoding</code>

## SHOWLANGUAGE

Displays the current language setting for the session.

Syntax	Example
<code>quote showlanguage</code>	<code>quote showlanguage</code>



---

# Globalization Support

This appendix provides information about Oracle Files globalization support. Topics include:

- [Globalization Support Overview](#)
- [The Repository](#)
- [Oracle Files Protocols](#)
- [Character Sets Supported in Oracle Files](#)
- [Languages Supported In Oracle Files](#)

## Globalization Support Overview

Oracle Files globalization support enables users to store and search documents of heterogeneous character sets and languages in a single Oracle Files 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.

## The Repository

The repository is the implementation of the core of Oracle Files, on which the protocol servers and applications are built. Globalization support is provided in the repository so that the other dependent components can share and utilize 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 on these documents.

## How to Choose the Database Character Set for Oracle Files

In the repository, all metadata strings, such as the name of the document or the description, are stored in the VARCHAR2 data type of the Oracle9i 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 the Oracle9i 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 a document's content is indexed, the BLOB data is converted from

the content's character set to the database character set for creation of the index text tokens. If the content's character set is not a subset of the database character set, 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 should be considered when selecting the database character set.

If your Oracle Files instance will contain multilingual documents, UTF-8 is the recommended database character set. UTF-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 which 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. UTF-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 UTF-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.

The Oracle9i database introduces the new character set, AL32UTF-8. In Release 1, AL32UTF-8 was the default character set for Unicode 3.0 deployment. In Release 2, AL32UTF-8 is compliant to the latest Unicode 3.1 standard, which contains the supplementary characters, particularly additional Chinese, Japanese, and Korean ideographs. AL32UTF-8 is the default character set of an Oracle9i database installation.

---

**Note:** Oracle Files does not support an AL32UTF-8 database because Oracle Text does not support Chinese, Japanese, and Korean lexers on an AL32UTF-8 database. UTF-8 is the recommended database character set for an Unicode-based file system. If Oracle Files is installed in an AL32UTF-8 database, Chinese, Japanese, and Korean documents will not get indexed and, thus, will not be searchable.

The Oracle Files Configuration Assistant will fail in a Chinese, Japanese, or Korean locale against an AL32UTF-8 database. This is because Oracle Text behaves differently when the database session language is initialized to an Asian language as opposed to American. JDBC initializes the database session language according to the locale of the running application, which in this case is the configuration tool.

---

## How to Make Sure Documents Are Properly Indexed in Oracle Files

To support documents in different character sets and languages in a single file system, the repository associates two globalization attributes per 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 upon insertion of a document, the repository determines a default character set as follows: the character set of the user's LibrarySession stored in the Localizer object is first used. This is obtained from the user's PrimaryUserProfile information at initialization of the user's LibrarySession.

## 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. Oracle Text's multilexer feature 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. They are defined as follows:

**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
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	N/A
Korean	KOREAN_LEXER	N/A
Latin American	BASIC_LEXER	BASE LETTER
Spanish Portuguese	BASIC_LEXER	BASE LETTER
Simplified Chinese	CHINES_VGRAM_LEXER	N/A
Swedish	BASIC_LEXER	BASE LETTER SWEDISH ALTERNATE SPELLING
Tradition Chinese	CHINESE_VGRAM_LEXER	N/A
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 have not been supported by Oracle Text are parsed as English. Oracle Files uses

the multilexer feature of Oracle Text. It is a global lexer containing German, Danish, Swedish, Japanese, Simplified Chinese, Traditional Chinese, and Korean sublexers.

If no language is specified upon insertion of a document, 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 LibrarySession. During initialization of the LibrarySession, the default language is obtained from the user's PrimaryUserProfile.
3. The defaults for both language and character set is specified by the Subscriber Administrator when a new user is created.

Oracle Files identifies languages using Oracle NLS language abbreviations. See ["Languages Supported In Oracle Files"](#) on page G-7 for a list of Oracle Files-supported languages.

### Service Configuration Properties

There are two service configuration properties that hold default character set and language values for Oracle Files Subscribers. The properties are:

- `IFS.SERVICE.DefaultCharacterSet`
- `IFS.SERVICE.DefaultLanguage`

These two properties are initialized with the Oracle Files Configuration Assistant tool and can be later modified through the Oracle Enterprise Manager Web site. The Oracle Files default character set should be the same or a subset of the database character set. The character set should be specified in accordance with the IANA standard naming convention. The language should be specified in accordance with Oracle naming for languages. See ["Character Sets Supported in Oracle Files"](#) on page G-5 and ["Languages Supported In Oracle Files"](#) on page G-7 for a list of Oracle Files-supported character sets and languages.

## Oracle Files Protocols

Oracle Files does not support multibyte user names for certain protocols. Access through WebDAV (Web Folders and Oracle FileSync), HTTP, and SMB 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.

### FTP

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, the Oracle Files FTP server provides the following QUOTE commands:

- **Ftp> quote setcharencoding:** Allows users to specify the character set for the FTP session. This character set specifies the character encoding to be used in subsequent FTP commands and the character set of the documents to be uploaded. 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.

- **Ftp> quote showcharencoding:** Displays the current character set of the FTP session. The character set is displayed in the IANA naming standards.
- **Ftp> quote setlanguage:** Allows users to specify the language for the FTP session. The language of a 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. Oracle language names should be used.
- **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 actually updates the settings in the Localizer object of the current LibrarySession. Subsequently, since quote commands cannot be issued until a 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. [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.

## SMB

The Server Message Block (SMB) protocol server implements the SMB protocol to allow mounting of Oracle Files as a disk drive in Microsoft Windows Explorer. Microsoft has included Unicode support for the SMB protocol since LanManager Version 0.12.

The SMB protocol does not allow users to pass the character set and language information to the server. The session defaults will be used for documents inserted into the repository via the SMB protocols.

## Character Sets Supported in Oracle Files

The following table summarizes the character sets supported in Oracle Files.

**Table G-2 Character Sets Supported in Oracle Files**

Language	IANA Preferred MIME Charset	IANA Additional Aliases	Java Encodings	Oracle Charset
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

**Table G–2 (Cont.) Character Sets Supported in Oracle Files**

Language	IANA Preferred MIME Charset	IANA Additional Aliases	Java Encodings	Oracle Charset
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 (Windows)	GBK	windows-936	GBK	ZHS16GBK
Chinese Traditional	big5	csbig5, x-x-big5	Big5	ZHT16BIG5
Chinese Traditional	windows-950	none	MS950	ZHT16MSWIN950
Chinese Traditional (EUC-TW)	EUC-TW	none	EUC_TW	ZHT32EUC
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

**Table G–2 (Cont.) Character Sets Supported in Oracle Files**

Language	IANA Preferred MIME Charset	IANA Additional Aliases	Java Encodings	Oracle Charset
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
Universal (UTF-8)	utf-8	unicode-1-1-utf-8, unicode-2-0-utf-8, x-unicode-2-0-utf-8	UTF8	UTF8
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

## Languages Supported In Oracle Files

The following table summarizes the languages supported in Oracle Files.

**Table G–3 Languages Supported in Oracle Files**

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

**Table G-3 (Cont.) Languages Supported in Oracle Files**

Oracle Language Name	Java Locale	ISO Locale
English	en_GB	en-gb
Estonian	et	et
Finnish	fi	fi
French	fr	fr
German	de	de
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

---

---

# Index

## A

---

- Access Control List Index Agent, C-2
- ACL cache, B-2
- administration login page, 3-4, 3-6, 4-5
- administration tools
  - administration tabs in Oracle Files, 4-5
  - Bulk NFS, 2-9
  - Bulk User Administration, 4-7
  - Bulk Workspace Administration, 4-8
  - Grid Control, 1-11, 4-4
  - Oracle Directory Manager, 3-7
  - Oracle Enterprise Manager Web site, 1-11, 4-2
  - Oracle Files Configuration Assistant, 4-1
- administrative accounts
  - ias\_admin, 3-2
  - orcladmin, 3-2
  - site\_admin, 3-2
  - Subscriber Administrator, 3-2
  - sysman, 4-4, 7-6
  - system, 3-2
- administrative roles, 3-1
- administrators
  - Site, 1-7, 3-2, 3-4
  - Subscriber, 1-6, 1-7, 3-2, 3-6
  - System, 1-7, 3-1, 3-3
  - workspace, 1-7
- Advanced Queueing
  - See* Oracle Advanced Queueing
- AFP
  - about, 2-1
  - access, 2-3
  - security issues, 8-1
- agents
  - about, 1-5
  - Access Control List Index, C-2
  - Dangling Object AV Cleanup, C-3
  - Event Exchanger, C-4
  - Expiration, C-5
  - Files Archive File to BFILE, 9-2, C-7
  - Files Delayed Archive File to BFILE, 9-2, C-7
  - Files OID User Synchronization, 3-7, C-7
  - Files Review Process Expiration, C-7
  - Files Subscriber Expiration, C-7
  - Files Subscriber Usage, C-7
  - Files Subscriber Usage Stats, C-8

- Files User Expiration, C-8
- Files Workflow Lock Cleanup, C-8
- Folder Index Analyzer, C-8
- Garbage Collection, C-9
- Inbound Queue Listener, C-9
- Lock, C-9
- Print, C-13
- Quota, C-13
- Service Warmup, C-13
- Service Watchdog, B-2, C-14
- analyze.sql script, 9-3, 11-1
- AppleTalk Filing Protocol
  - See* AFP
- AQ
  - See* Oracle Advanced Queueing
- Archive, 3-9
- archiving
  - data, 9-2
  - features, 3-9
- authentication
  - case-sensitive, B-4
  - NIS, 2-11
  - user, 1-13, 8-1
- autoprovisioning, 3-8

## B

---

- BACKGROUND\_DUMP\_DEST parameter, A-3
- backups, 9-1
- BFILE
  - archiving, 9-2
  - base path, 9-2
  - definition, 9-2
  - disabling archiving, 9-2
  - relative path, 9-2
- Binary Large Object
  - See* BLOB
- blaf.xss style sheet, 10-2
- BLOB
  - about, 9-1
  - Index, 9-5
  - space utilization, 9-5
- BlockOverhead, 9-4
- branding, 10-1
- browser-based access, 2-3
- Bulk Administration tools

- about, 4-6
- NFS, 2-9
- running, 4-6
- User Administration, 4-7
- Workspace Administration, 4-8

## C

---

- caches
  - ACL, B-2
  - Committed Data, 6-10
  - maximum size, B-4
- cancel event, 10-6
- categories
  - about, 1-8
  - creating, 3-9
  - deleting, 3-9
  - managing, 3-9
  - modifying, 3-9
- character set, default, B-1
- chunks, 9-4
- ClearContextJobs.sql, A-3
- client
  - access paths, 2-2
  - certification information, 2-2
  - load balancing, D-2
  - platforms, 2-3
- clients
  - about, 2-2
  - FTP, 2-4
  - HTTP, 2-3
  - Hummingbird Maestro, 2-6
  - installing, 2-2
  - Macintosh, 2-3
  - NFS, 2-4
  - Oracle FileSync, 2-2, 2-3
  - SMB/NTFS, 2-4
  - WebDAV, 2-1, 2-3
- cluster, 1-10, D-1
- cn=orcladmin account, 3-2
- colors, changing in the Oracle Files interface, 10-1
- command-line utilities
  - dcmctl, 4-5, 5-6
  - emctl, 4-5
  - ifsbulkadmintools, 4-5
  - ifsca, 4-5
  - ifsctl, 5-8
  - opmnctl, 4-5
- Committed Data Cache
  - about, 6-10
  - configuration properties, 6-11
  - dynamically changing, 6-11
- concurrent sessions
  - See sessions
- configuration
  - domain properties, 6-1
  - node, 5-6, 6-3
  - Oracle Files, 4-1
  - server, 6-13
  - service, 6-8

- connect time failover, D-3
- connection pools
  - read-only, 6-10
  - writable, 6-10
- connections, minimum number of, 6-12
- Content Garbage Collection Agent, 11-2
- content, migrating, E-1, E-2
- Cost-Based Optimizer, 9-3
- CreateContextFunnelProcedure.SQL, A-2
- CreateContextIndex.sql, A-2
- CreateContextPreferences.sql, A-2
- credential manager
  - Oracle Internet Directory, 1-4, 1-6
  - selecting, 4-1
  - service configuration properties, B-4
  - settings, 6-8
- credentials
  - types of, 1-6
  - user, 8-1
- ctx\_ddl.optimize\_index, A-2
- ctx\_ddl.sync\_index, A-2
- custom workflows
  - about, 10-4
  - deleting, 10-8
  - editing, 10-7
  - registering, 10-7
- customization
  - branding, 10-1
  - changing title bar text, 10-3
  - changing Web UI colors, 10-1
  - changing Web UI fonts, 10-2
  - changing Web UI images, 10-2
  - limitations, 10-3
  - types of, 10-1
- custom.xss style sheet, 10-1, 10-2

## D

---

- Dangling Object AV Cleanup Agent, C-3
- data
  - archiving, 9-2
  - backing up, 9-1
- data cache, maximum size, B-4
- data types, standard, 1-10
- database
  - backing up, 9-1
  - clustering, 1-10
  - failover, 1-10
  - listeners, D-2
  - tables, 1-10
- DAV
  - See WebDAV
- DBConnectDescriptor parameter, D-8
- DBMS\_JOBS
  - about, A-3
  - changing or removing, A-3
  - monitoring, A-3
- dcmctl script, 4-5, 5-6
- default
  - character set, B-1

- language, 3-7, B-1
- default settings, specifying, 3-6
- deployment, 1-4
- DHCP, 2-3
- directories, migrating to Oracle Files, E-3
- Distributed Authoring and Versioning
  - See* WebDAV
- document
  - overhead, 9-6
  - storage information, 7-2
- documents
  - associating formats with, 6-20
  - designating to be indexed, A-4
- domain
  - about, 5-1
  - adding middle tiers, 4-1
  - creating, 4-1
  - diagram, 1-2
  - fully-qualified name, 5-1
  - monitoring performance, 7-1
  - refreshing, 5-3
  - starting and stopping, 5-2
  - starting from command line, 5-8
  - statistics, 7-1
  - stopping, 5-3
- domain controller
  - about, 5-1
  - checking status of, 5-2
  - log file, 6-2, 7-4
  - migrating to a new host, 5-4
  - migrating to an existing host, 5-4
  - setting up, 4-1
- domain properties
  - about, 6-1
  - changing, 6-1
- DTD
  - for User Administration tool, 4-7
  - for Workspace Administration tool, 4-9

## E

---

- .EAR file, 1-11
- edit-in-place, 1-9
- emctl script, 4-5
- Event Exchanger Agent, C-4
- event subscriptions, 10-6
- events
  - cancel, 10-6
  - creating in Oracle Workflow, 10-6
  - launch, 10-5
  - process status, 10-6
  - response, 10-6
- Expiration Agent, C-5
- Explain Plan, 9-6

## F

---

- failover
  - about, 1-10, D-2
  - connect time, D-3

- transparent application, D-4
- Federated Search
  - See* Oracle Collaboration Suite Search
- File Transfer Protocol
  - See* FTP
- files
  - categories, 1-8
  - designating to be indexed, A-4
  - drag and drop, E-3
  - .EAR, 1-11
  - editing in place, 1-9
  - FTP to Oracle Files, E-2
  - .Jar, 1-11
  - locking and unlocking, 3-10
  - migrating, E-2, E-3
  - restoring, 3-10
  - reviewing, 1-8
  - synchronizing, 1-9
  - versioning, 1-8
  - .WAR, 1-11
- Files Archive File to BFILE Agent, 9-2, C-7
- Files Base Server Configuration, C-6
- Files Delayed Archive File to BFILE Agent, 9-2, C-7
- Files OID User Synchronization Agent, 3-7, C-7
- Files Review Process Expiration Agent, C-7
- Files Subscriber Expiration Agent, C-7
- Files Subscriber Usage Agent, C-7
- Files Subscriber Usage Stats Agent, C-8
- Files User Expiration Agent, C-8
- Files Workflow Lock Cleanup Agent, C-8
- FilespageLayout.uit file, 10-3
- Files-specific server configuration, C-7
- Folder Index Analyzer Agent, C-8
- folders, migrating, E-2
- fonts, changing in the Oracle Files interface, 10-2
- formats
  - about, 6-20
  - default, 6-21
- FTP
  - about, 2-1
  - access, 2-4
  - benefits of, 2-4
  - files into Oracle Files, E-2
  - port, C-6
  - quote commands, F-1
  - security issues, 8-1
  - server configuration parameters, C-5
  - troubleshooting, 11-2, 11-3

## G

---

- garbage collection, 9-7
- Garbage Collection Agent, C-9
- GrantContextToIFS.sql, A-2
- Grid Control
  - about, 1-11, 4-4
  - accessing, 4-4, 7-6
  - configuring for Oracle Files, 1-11, 7-6
  - editing metric collection intervals, 7-8
  - editing metric thresholds, 7-8

- logs, 7-4
- Management Agent, 1-11, 4-4, 7-5
- security issues with, 8-2
- settings for Real Application Clusters, D-7
- viewing Oracle Files metrics, 7-7

groups, migrating, E-1

guest account, 6-2

## H

---

hardware requirements, 1-3

high availability, D-5

HSM system, 9-2

HTTP

- about, 2-1
- access, 2-3
- security issues, 8-2

HTTP nodes

- about, 5-1
- creating, 6-6
- disabling, 5-6
- log files, 7-5
- starting, 5-5
- stopping, 5-5

httpd.conf file, 6-23

Hummingbird Maestro

- about, 2-6
- command-line options, 2-7
- error messages, 2-8
- linking directories, 2-7

Hypertext Transfer Protocol

*See* HTTP

## I

---

ias\_admin account, 3-2

IFS\_TEXT index

- about, A-1
- maintaining, A-2
- optimizing, A-2
- refreshing, A-2

ifsctl

- log file, 7-5
- script, 5-8
- syntax, 5-8

IfsPasswordApplications parameter, 8-2

images, changing in the Oracle Files interface, 10-2

Inbound Queue Listener Agent, C-9

Indexed Medias tablespace, 9-4

indexing

- setting up, 6-20, A-4
- troubleshooting, A-5
- with Oracle Text, A-1

interconnect, D-1

interMedia Text, A-1

## J

---

.JAR files, 1-11

Java

- cache statistics, 9-7

- heap size, 11-1
- servlets, 1-11
- Xmx settings, 9-7

Java Server Pages (JSPs), 1-11

JDBC, 8-3, B-5

JOB\_QUEUE\_PROCESSES parameter, A-3, D-6

## L

---

language

- default, B-1
- display, 3-7

Large Objects

*See* LOBs

launch event, 10-5

LDAP, 1-13

LIBRARYOBJECTS, B-4

listeners

- about, D-2
- load balancing, D-4

load balancing

- about, D-2
- client, D-2
- disabling during configuration, D-7
- listener, D-4

LOBs, 1-10, 9-1

Lock Agent, C-9

log files

- domain controller, 6-2, 7-4
- Grid Control, 7-4
- HTTP node, 7-5
- ifsctl, 7-5
- Oracle Enterprise Manager Web site, 7-4
- Oracle Files Configuration Assistant, 7-5
- regular node, 6-4, 7-4
- setting options, 7-5

logos, changing in the Oracle Files interface, 10-2

## M

---

Macintosh

- clients, 2-3
- Go menu, 2-3

Management Agent

- about, 1-11
- installing, 4-4, 7-5

mapping network drives, 2-1, 2-4

MAX\_COMMIT\_PROPAGATION\_DELAY

- parameter, D-6

memory, monitoring, 7-2

metadata

- deleted during migration, E-2
- storage, 1-10

metrics

- about, 1-12
- changing collection behavior, 7-6
- editing collection intervals, 7-8
- editing thresholds, 7-8
- Run Load Balancer Response Time, 7-7
- Run Repos, 7-7



- Run Response Time, 7-7
- viewing in Grid Control, 7-7
- middle tiers
  - adding to the domain, 4-1
  - deployment considerations, 1-4
- migrating
  - data, E-3
  - domain controller, 5-4
- migration
  - content, E-1, E-2
  - file, E-2
  - folder, E-2
  - group, E-1
  - metadata, E-2
  - user, E-1
- MIME types, 6-20, A-4
- monitoring
  - memory, 7-2
  - metrics, 7-5
  - sessions, 7-2
  - threads, 7-2
  - vmstat tool, 11-1
- mounting remote file systems, 2-1

## N

---

- NB server
  - See* NetBIOS protocol
- near-line storage, 9-2
- NetBIOS protocol
  - about, C-9
  - server configuration parameters, C-9
- network channel encryption, 8-2
- Network File System
  - See* NFS
- NFS
  - about, 2-1, 2-4
  - general limitations, 2-5
  - Hummingbird Maestro clients, 2-6
  - mounting, 2-5
  - server configuration parameters, C-10
  - troubleshooting, 11-2
  - trusted client list, 2-10
  - UIDs, 2-9, 6-3
  - versioning limitations, 1-5
- NIS authentication, 2-11
- node
  - access control level, 6-3
  - diagram, 1-3
  - guardian process, 1-3
  - Java command, 6-3
  - log files, 6-4, 7-4
  - manager, 1-3
  - statistics, 7-3
- node configurations
  - about, 5-6, 6-3
  - adding servers, 6-4, 6-6
  - adding services, 6-4, 6-5
  - changing, 6-3
  - creating, 6-5, 6-6

- deleting, 6-7
- nodes
  - about, 5-1
  - checking status of, 5-2
  - HTTP, 1-2, 5-1
  - making active or inactive, 6-3
  - monitoring performance, 7-3
  - RAC, D-1
  - regular, 1-2, 5-1
  - setting up, 4-1
  - starting, 5-5
  - starting from command line, 5-8
  - stopping, 5-5
- Non-Indexed Medias tablespace, 9-4
- Notification Mailer
  - program, 10-10
  - sample configuration file, 10-10
  - setting up, 10-9
  - starting, 10-11
  - tag file, 10-10
- notifications
  - e-mail, 10-8
  - workflow, 1-13
- NT File System
  - See* NTFS
- NTFS
  - about, 2-1
  - access, 2-4
  - log levels, 6-4
  - server configuration parameters, C-12
  - troubleshooting, 11-3
  - versioning limitations, 1-5

## O

---

- OC4J
  - about, 1-11
  - deploying, 6-6
  - managing, 5-9
- OC4J\_DAS, 3-7
- off-line storage, 9-2
- Op Locks, C-15
- OPMN
  - See* Oracle Process Management and Notification
- opmnctl script, 4-5, 5-9
- Optimize Job, A-3
- Oracle Advanced Queueing, 1-10, 10-4
- Oracle Advanced Security, 8-3
- Oracle Collaboration Suite Search
  - about, 1-8, 6-17
  - configuration parameters, 6-18
  - setting up, 6-18
- Oracle Content Management SDK, 1-1
- Oracle Directory Manager, 3-7, 4-5, 8-9
- Oracle Email, 6-17
- Oracle Enterprise Manager
  - about, 1-11
  - diagrams, 1-12
  - starting and stopping, 4-3
- Oracle Enterprise Manager Web site

- about, 4-2
- accessing, 4-3
- logs, 7-4
- security issues with, 8-2
- troubleshooting, 11-3
- Oracle Files
  - about, 1-1
  - administration tabs, 4-5
  - architecture, 1-1
  - configuring, 4-1
  - configuring for RAC, D-1
  - customization, 10-1
  - domain, 1-2, 5-1
  - features, 1-6
  - HTTP nodes, 1-2
  - log files, 7-4
  - metrics, 1-12
  - nodes, 1-2
  - printing from, 6-19
  - processes, 5-1
  - protocols, 2-1
  - running on port 80, 6-22
  - schema, 1-2, 1-10, 4-1
  - security, 8-1
  - starting, 5-2
  - target type, 7-6
  - URL, 2-3
- Oracle Files Configuration Assistant
  - about, 4-1
  - log, 7-5
  - running, 4-2
- Oracle Files-specific password
  - about, 8-2
  - changing protocols that use, 8-2
- Oracle FileSync
  - about, 1-9
  - access, 2-3
  - installing, 2-2
  - token credential, 8-3
- Oracle HTTP Server
  - changing the port number, 6-23
  - configuring for SSL, 8-3
  - restarting, 6-24
- Oracle Internet Directory
  - about, 1-6, 1-13
  - configuring for SSL, 8-3, 8-5
  - creating users in, 3-8
  - installation recommendations, 1-4
  - required user attributes, 11-2
  - security issues with, 8-3
- Oracle Management Agent
  - See* Management Agent
- Oracle Process Management and Notification, 5-9
- Oracle Text
  - about, 1-10, A-1
  - maintaining the IFS\_TEXT index, A-2
  - tablespaces, A-1
  - troubleshooting, A-5
- Oracle Text Data tablespace, A-1
- Oracle Text Index tablespace, A-2

- Oracle Text Keymap tablespace, A-1
- Oracle Ultra Search, 6-17
- Oracle Voicemail & Fax, 6-17
- Oracle Workflow
  - about, 1-8, 1-13
  - changing the port number, 6-22
  - integrating with Oracle Files, 10-4
  - Notification Mailer, 10-9
  - schema name, 6-2
  - setting up e-mail notifications, 10-8
- Oracle Workflow Builder, 1-9, 1-13, 10-4
- Oracle9i Application Server
  - about, 1-11
  - scripts, 4-5
- Oracle9i Database, 1-10
- Oracle9i Real Application Clusters
  - See* Real Application Clusters
- Oracle9iAS Containers for J2EE
  - See* OC4J
- Oracle9iAS Portal, setting URLs in, 8-4
- Oracle9iAS Single Sign-On
  - changing Oracle Files URLs in, 8-4
  - limitations, 1-6, 3-4
  - registering ports with, 6-23
- Oracle9iAS Web Cache
  - changing the port number, 6-23
  - starting, 6-23
- oracle.ifs.files.cancel, 10-6
- oracle.ifs.files.response, 10-6
- oracle.ifs.files.review, 10-5
- orcladmin account, 3-2
- orphan session, B-2
- out-of-memory exception, 11-1

## P

---

- passwords
  - case-sensitive, B-4
  - changing the schema password, 8-8
  - changing the system password, 8-7
  - limitations, 3-8
  - Oracle Files-specific, 8-2
  - resetting, 3-5
- PCTVERSION parameter, 9-5
- performance
  - monitoring domain, 7-1
  - monitoring node, 7-3
  - troubleshooting, 9-6
  - tuning, 9-3
- portal home page, 1-10
- ports
  - AFP, C-3
  - application, C-6
  - FTP, C-6
  - NFS, C-11
  - registering with Single Sign-On, 6-23
  - running Oracle Files on port 80, 6-22
  - SMB, C-15
- Print Agent, C-13
- printers

- adding, 6-19
  - deleting, 6-19
- printing from Oracle Files, 6-19
- privacy statement, C-6
- process status event, 10-6
- processes
  - node, 5-5
  - starting and stopping, 5-3
- properties
  - changing domain configuration, 6-1
  - domain, 6-1
- protocol servers
  - about, 2-1
  - AFP, 2-1
  - FTP, 2-1, 2-4, C-5
  - HTTP, 2-1, 2-3
  - NetBIOS, C-9
  - NFS, 2-1, 2-4, C-10
  - NTFS, 2-1, 2-4, C-12
  - Oracle Files-specific passwords, 8-2
  - security, 8-1
  - selecting, 4-1
  - SMB, 2-1, 2-4, C-14, E-3
  - WebDAV, 2-1, 2-3, C-4
- protocols
  - and DHCP, 2-3
  - supported, 2-3
  - versioning limitations, 1-5
- provisioning
  - troubleshooting, 11-2
  - user, 1-13
- Public folder
  - disabling, 3-7
  - enabling, 3-7

## Q

---

- Quota Agent, C-13
- quotas
  - increases in, 3-9
  - user, C-13
  - workspace, 1-7, 3-7, 3-10
- quote commands, F-1

## R

---

- RAC
  - See* Real Application Clusters
- Read-Only Connection Pool
  - about, 6-10
  - configuration properties, 6-12
  - dynamically changing, 6-11
  - parameters, B-3
- Real Application Clusters
  - about, 1-10, D-1
  - configuration tasks, D-7
  - connect descriptor settings, D-5
  - post-configuration tasks, D-7
  - preconfiguration tasks, D-6
  - settings for Grid Control, D-7

- Redo log size, 11-2
- registry.xml file, D-4, D-5, D-7
- regular nodes
  - about, 5-1
  - log file, 7-4
  - starting, 5-5
  - stopping, 5-5
- response event, 10-6
- restoring files, 3-10
- review process
  - approver, 1-8
  - custom, 1-9
  - reviewer, 1-9
  - submitting for review, 1-9

## S

---

- schema
  - \$CM, 9-1
  - \$DR, 9-1
  - \$ID, 9-1
  - changing the password, 8-8
  - creating, 4-1
  - Oracle Files, 1-2, 1-10
  - tables, 1-10
  - workflow, 6-2
- scripts
  - analyze.sql, 9-3
  - dcmctl, 4-5, 5-6
  - emctl, 4-5
  - group creation, E-1
  - ifsbulkadmintools, 4-5
  - ifscs, 4-2, 4-5
  - ifscctl, 4-5, 5-8
  - opmnctl, 4-5, 5-9
  - SQL, A-2, A-3, A-4
- searches
  - advanced, 1-8
  - category, 1-8
  - Oracle Collaboration Suite, 1-8, 6-17
  - simple, 1-8
- searching
  - specifying search timeout period, A-5
  - troubleshooting, A-5
- security
  - issues with administration interfaces, 8-2
  - issues with AFP, 8-1
  - issues with FTP, 8-1
  - issues with HTTP, 8-2
  - issues with JDBC, 8-3
  - issues with Oracle Internet Directory, 8-3
  - issues with WebDAV, 8-2
  - network channel encryption, 8-2
- Sendmail
  - setting up, 10-8
  - starting, 10-8
  - testing configuration of, 10-9
- server configuration
  - Files Base, C-6
  - properties, C-1

- viewing inherited properties, 6-15
- server configurations
  - about, 6-13
  - abstract and non-abstract, 6-14
  - creating, 6-15
  - deleting, 6-17
  - Files-specific, C-7
- Server Message Block
  - See* SMB
- servers
  - about, 1-5
  - adding to node, 6-4, 6-6
  - loading and unloading, 5-7
  - protocol, 2-1
  - setting Initially Started, 6-4
  - slow read and write activity, 11-1
  - starting, 5-6
  - stopping, 5-6
- service configuration
  - access levels, 6-9
  - properties, B-1
  - types, 6-8
- service configurations
  - about, 6-8
  - changing, 6-8
  - creating, 6-9
  - default, 6-2
- Service Warmup Agent, C-13
- Service Watchdog Agent, B-2, C-14
- services
  - about, 1-5
  - adding to node, 6-4, 6-5
  - changing at runtime, 6-10
  - default character set, 6-8
  - default language, 6-8
  - failed, B-2
  - specifying automatic shutdown, 6-10
- servlets, Java, 1-11
- session
  - service configuration properties, B-5
  - time-out period, B-2
- sessions
  - comparing server types, 7-2
  - enabling and disabling acceptance of, 6-10
  - monitoring, 7-2
  - number of concurrent, 6-10, B-1
  - number of connected, 7-2
  - orphan, B-2
  - viewing by server type, 7-2
- SetupContextJobs.sql, A-3
- silent configuration, 4-2
- Single Sign-On
  - See* Oracle9iAS Single Sign-On
- site administration interface, 3-4
- Site Administrator, 1-7, 3-2, 3-4
- site\_admin account, 3-2
- sizing guidelines, 1-3
- SMB
  - about, 2-1
  - access, 2-4
  - for migrating data, E-3
  - IP address, C-15
  - port, C-15
  - printing through, 6-19
  - server configuration parameters, C-14
  - troubleshooting, 11-2
  - versioning limitations, 1-5
- SQL scripts
  - ClearContextJobs.sql, A-3
  - CreateContextFunnelProcedure.SQL, A-2
  - CreateContextIndex.sql, A-2
  - CreateContextPreferences.sql, A-2
  - GrantContextToIFS.sql, A-2
  - SetupContextJobs.sql, A-3
  - SyncContextIndex.sql, A-4
  - ViewContextErrors.sql, A-4
  - ViewDocumentByRowID.sql, A-4
- SSL
  - configuring Oracle HTTP Server with, 8-3
  - using Oracle Files with, 8-3
  - using Oracle Internet Directory with, 8-3, 8-5
- SSO
  - See* Oracle9iAS Single Sign-On
- statistics
  - data distribution, 9-3
  - domain, 7-1
  - Java cache, 9-7
  - node, 7-3
  - Subscriber, 3-5
- Statspack utility, 9-6
- storage
  - calculating, 9-4
  - document, 7-2
  - near-line, 9-2
  - off-line, 9-2
  - optimized, 1-10
- style sheets
  - blaf.xss, 10-2
  - custom.xss, 10-1, 10-2
- subscriber administration interface, 3-6
- Subscriber Administrator, 1-6, 1-7, 3-2, 3-6
- Subscriber Statistics page, 3-5
- Subscribers
  - about, 1-6
  - creating, 3-5
  - specifying archive settings, 3-5
  - specifying default settings, 3-6
  - specifying notification settings, 3-5
- Sync Job, A-3
- SyncContextIndex.sql, A-4
- sysman account, 4-4, 7-6
- system account
  - about, 3-2
  - changing the password, 8-7
  - encrypting the system password in targets.xml, 8-8
- System Administrator, 1-7, 3-1, 3-3

## T

---

- tables, database, 1-10
- tablespaces
  - Indexed Medias, 9-4
  - Non-Indexed Medias, 9-4
  - Oracle Files Primary, 9-6
  - Oracle Text Data, A-1
  - Oracle Text Index, A-2
  - oracle Text Keymap, A-1
- TAF
  - See* Transparent Application Failover
- target type for Oracle Files, 7-6
- targets.xml
  - encrypting the schema password in, 8-9
  - encrypting the system password in, 8-8
- TCP\_IP\_ABORT\_INTERVAL parameter, D-4
- TCP\_KEEPAIVE\_INTERVAL parameter, D-4
- text
  - analyzing, 1-10
  - indexing, 1-10
  - searching, 1-10
- threads, monitoring, 7-2
- title bar, changing text in, 10-3
- tnsnames.ora entries, D-3, D-6
- Transparent Application Failover, D-4
- trash management, 3-9

## U

---

- UIDs, 2-9, 6-3
- UNIX
  - Sendmail, 10-8
  - symbolic links, 9-2
  - UIDs, 2-9, 6-3
- upgrade issues, 8-7
- URLs
  - Back to Portal, C-6
  - Oracle Files, 2-3
  - Oracle FileSync, C-6
  - Oracle Workflow, C-6
  - Oracle9iAS Portal, 8-4
  - Single Sign-On, 6-24
  - SSO, 8-4
- User Administration tool
  - about, 4-7
  - DTD, 4-7
  - limitations, 4-7
  - sample XML file, 4-7
  - troubleshooting, 4-8
- user name limitations, 3-8
- users
  - authenticating, 1-5, 1-13, 8-1
  - creating, 3-7
  - deleting, 3-9
  - emailing, 3-8
  - enabling and disabling, 3-9
  - managing, 3-7
  - migrating, E-1
  - modifying user information, 3-8
  - provisioning, 1-13, 3-7

- quota, 3-9
- XML file for updating, 4-7

## V

---

- verbosegc, 9-7
- versioning, 1-8
- ViewContextErrors.sql, A-4
- ViewDocumentByRowID.sql, A-4
- vmstat, 11-1

## W

---

- .WAR file, 1-11
- Web Cache Manager, 6-23
- Web Folders
  - See* WebDAV
- WebDAV
  - about, 2-1
  - access, 2-3
  - clients, 2-1
  - security issues, 8-2
  - server configuration parameters, C-4
- web.xml file, C-8
- wfmail.cfg file, 10-10
- wfmail.snd file, 10-10
- wfmail.tag file, 10-10
- .wft
  - See* workflow process definition
- workflow
  - default process, 10-5
  - designer, 1-9, 1-13, 3-5, 10-4
  - notifications, 1-13
  - process URL, 10-5
  - schema name, 6-2
- workflow process definition
  - creating, 10-4
  - deleting, 10-8
  - editing, 10-7
  - registering, 3-5, 10-7
- workspace
  - access levels, 1-7
  - administrator, 1-7
  - folder settings, 3-7
  - participant, 1-7
  - quota, 1-7, 3-7, 3-10
  - viewer, 1-7
- Workspace Administration tool
  - about, 4-8
  - DTD, 4-9
  - sample XML file, 4-8
  - troubleshooting, 4-10
- workspaces
  - about, 1-7
  - administering, 3-10
  - XML file for creating/updating, 4-8
- Writable Connection Pool
  - about, 6-10
  - configuration properties, 6-13
  - dynamically changing, 6-11

parameters, B-3

## **X**

---

### XML file

for creating workspaces, 4-8

for updating users, 4-7

for updating workspaces, 4-8

### Xmx settings

about, 9-7

modifying, 11-1