

Oracle® Automatic Storage Management

Administrator's Guide

12c Release 1 (12.1)

E41058-11

May 2015

Primary Author: Eric Belden

Contributing Authors: Jerry Abraham, Prasad Bagal, Mark Bauer, Bill Bridge, Chan Chan, Xiaobin Chen, Hanlin Chien, Jonathan Creighton, Steve Fogel, Dave Friedman, Barb Glover, Fred Glover, Allan Graves, Shie-rei Huang, Rekha Iyer, Diane Lebel, Rich Long, Colin McGregor, Gregory Mengel, Harendra Mishra, Valarie Moore, Nitin Munjal, Darshan Nagarajappa, Harish Nandyala, Bob Nelson, Balaji Pagadala, Satish Panchumarthy, Soma Prasad, Kathy Rich, Harshavardhan Sabbineni, Francisco Sanchez, Santhosh Selvaraj, Ara Shakian, Duane Smith, Joshua Smith, Malai Stalin, Amar Subba, Yaser Suleiman, Elisabeth Thibault, Michael Timpanaro-Perrotta, Samarjeet Tomar, Brian Tsao, Nitin Vengurlekar, P Venkatraman, Anton Verhulst, Radek Vingralek, Ron Weiss, Ric Werme, Rajiv Wickremesinghe, Jim A. Williams, Sivakumar Yarlagadda, Song Ye, Krishnan Yegnashankaran, Jon Zolla

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xxvii
Audience	xxvii
Documentation Accessibility	xxvii
Related Documents.....	xxviii
Conventions.....	xxviii
Changes in This Release for Oracle Automatic Storage Management	
Administrator's Guide	xxix
Changes in Oracle Automatic Storage Management 12c Release 1 (12.1.0.2).....	xxix
New Features	xxix
Changes in Oracle Automatic Storage Management 12c Release 1 (12.1.0.1).....	xxx
New Features	xxx
Deprecated Features.....	xxxiv
Desupported Features	xxxiv
Changes in Oracle ACFS and Oracle ADVM for Oracle ASM 12c Release 1 (12.1.0.2)	xxxv
New Features	xxxv
Changes in Oracle ACFS and Oracle ADVM for Oracle ASM 12c Release 1 (12.1.0.1).....	xxxvi
New Features	xxxvii
Part I Introduction	
1 Introducing Oracle Automatic Storage Management	
Overview of Oracle Automatic Storage Management	1-1
About Oracle Automatic Storage Management Cluster File System	1-2
Understanding Oracle ASM Concepts	1-2
About Oracle ASM Instances.....	1-3
About Oracle ASM Disk Groups.....	1-5
About Mirroring and Failure Groups.....	1-5
About Oracle ASM Disks	1-6
About Oracle ASM Allocation Units	1-7
About Oracle ASM Files.....	1-7

Understanding Oracle ASM Disk Group Administration	1-11
About Discovering Disks	1-11
About Mounting and Dismounting Disk Groups	1-11
About Adding and Dropping Disks	1-11
About Online Storage Reconfigurations and Dynamic Rebalancing	1-12

2 Exploring Considerations for Oracle ASM Storage

Storage Resources for Disk Groups.....	2-1
Oracle ASM and Multipathing	2-3
Recommendations for Storage Preparation	2-4
Storage Device Path and Permission Persistence.....	2-5

Part II Oracle ASM Instances and Disk Groups

3 Administering Oracle ASM Instances

Operating with Different Releases of Oracle ASM and Database Instances Simultaneously	3-1
Initialization Parameters for Oracle ASM Instances.....	3-2
About Initialization Parameter Files for an Oracle ASM Instance	3-3
About Backing Up, Copying, and Moving an Oracle ASM Initialization Parameter File.....	3-4
About Oracle ASM Initialization Parameter Settings	3-6
About Automatic Memory Management for Oracle ASM.....	3-7
Recommended Settings for Oracle ASM Initialization Parameters	3-8
About Setting Database Initialization Parameters for Use with Oracle ASM	3-14
Administration of Oracle ASM Instances.....	3-15
Managing Oracle Flex ASM	3-15
Using Oracle Restart	3-21
About Starting Up an Oracle ASM Instance.....	3-21
About Shutting Down an Oracle ASM Instance	3-25
About Administering Oracle ASM Instances with Server Control Utility	3-27
About Out of Place Upgrades.....	3-27
About Configuring Oracle Grid Infrastructure with the Configuration Wizard.....	3-27
About Active Session History Sampling for Oracle ASM	3-28
About Oracle Home User on Windows	3-28
Upgrading and Patching Oracle ASM	3-28
About Oracle ASM Rolling Upgrade.....	3-29
About Oracle ASM Rolling Patches	3-30
About Converting to Oracle Flex ASM	3-30
Oracle ASM Filter Driver	3-33
About Oracle ASM Filter Driver	3-34
Deciding Between Oracle ASMLIB and Oracle ASM Filter Driver.....	3-35
Configuring Oracle ASM Filter Driver.....	3-36
About Migrating to Oracle ASM Filter Driver From ASMLIB	3-38
Determining Whether Oracle ASM Filter Driver Has Been Configured	3-41

Updating the Oracle ASM Filter Driver AFD_DISKSTRING Parameter	3-41
Updating the Oracle ASM ASM_DISKSTRING Parameter for Oracle ASM Filter Driver Disks	3-42
Setting, Clearing, and Scanning Oracle ASM Filter Driver Labels	3-42
Deconfiguring Oracle ASM Filter Driver	3-43
Authentication for Accessing Oracle ASM Instances	3-46
About Privileges for Oracle ASM.....	3-47
Creating Users with the SYSASM Privilege	3-50
Operating System Authentication for Oracle ASM	3-51
Password File Authentication for Oracle ASM	3-51
Managing a Shared Password File in a Disk Group	3-52
Migration of a Database to Use Oracle ASM	3-54
About Using Oracle Recovery Manager to Migrate Databases to Oracle ASM.....	3-55
Best Practices White Papers on Migrating to Oracle ASM	3-55

4 Administering Oracle ASM Disk Groups

Managing Disk Group Attributes	4-2
About Viewing and Setting Disk Group Attributes.....	4-2
Summary of Disk Group Attributes	4-2
Creating Disk Groups	4-7
Using the CREATE DISKGROUP SQL Statement.....	4-7
Creating Disk Groups for Data and Fast Recovery Area	4-9
Creating Disk Groups for a New Oracle Installation	4-10
Specifying the Sector Size for Drives	4-11
Storing Oracle Cluster Registry and Voting Files in Oracle ASM Disk Groups	4-13
Altering Disk Groups	4-15
Managing Oracle ADVM Volumes in a Disk Group	4-16
Adding Disks to a Disk Group	4-16
Using the ALTER DISKGROUP SQL Statement to Add Disks to a Disk Group	4-17
Replacing Disks in Disk Groups	4-18
Renaming Disks in Disk Groups	4-18
Dropping Disks from Disk Groups.....	4-19
Intelligent Data Placement	4-20
Resizing Disks in Disk Groups	4-21
Undropping Disks in Disk Groups	4-21
Manually Rebalancing Disk Groups.....	4-21
Tuning Rebalance Operations	4-23
Scrubbing Disk Groups	4-24
Oracle ASM Disk Discovery	4-25
How A Disk is Discovered	4-25
Disk Discovery Rules	4-26
Improving Disk Discovery Time	4-27
Managing Capacity in Disk Groups.....	4-27

Negative Values of USABLE_FILE_MB	4-29
Oracle ASM Mirroring and Disk Group Redundancy	4-29
Mirroring, Redundancy, and Failure Group Options	4-30
Oracle ASM Recovery from Read and Write I/O Errors	4-33
Oracle ASM Fast Mirror Resync.....	4-34
Even Read for Disk Groups	4-36
Preferred Read Failure Groups	4-37
Performance and Scalability Considerations for Disk Groups	4-38
Determining the Number of Disk Groups	4-38
Performance Characteristics When Grouping Disks	4-39
Oracle ASM Storage Limits.....	4-39
Disk Group Compatibility	4-40
Overview of Disk Group Compatibility	4-41
Disk Group Compatibility Attributes	4-41
Setting Disk Group Compatibility Attributes	4-42
Features Enabled By Disk Group Compatibility Attribute Settings	4-46
Considerations When Setting Disk Group Compatibility in Replicated Environments	4-48
Managing Oracle ASM File Access Control for Disk Groups	4-49
About Oracle ASM File Access Control	4-49
Setting Disk Group Attributes for Oracle ASM File Access Control	4-50
Using SQL Statements to Manage Oracle ASM File Access Control	4-51
Maintaining Disk Groups	4-53
Mounting and Dismounting Disk Groups	4-54
Mounting Disk Groups Using the FORCE Option.....	4-54
Checking the Internal Consistency of Disk Group Metadata	4-55
Dropping Disk Groups	4-56
Renaming Disks Groups.....	4-57

5 Administering Oracle ASM Files, Directories, and Templates

What Types of Files Does Oracle ASM Support?.....	5-1
About Oracle ASM File Names.....	5-2
Single File Creation Form.....	5-4
Multiple File Creation Form	5-4
Fully Qualified File Name Form	5-4
Alias Oracle ASM File Name Forms.....	5-6
Creating a Tablespace in Oracle ASM: Using a Data File with an Alias Name	5-6
Alias Oracle ASM File Name with Template Form.....	5-7
Incomplete Oracle ASM File Name Form.....	5-7
Incomplete Oracle ASM File Name with Template Form.....	5-8
Creating and Referencing Oracle ASM Files in the Database	5-8
Creating Oracle ASM Files Using a Default File Location for Disk Group Specification.....	5-8
Using Oracle ASM File Names in SQL Statements	5-9
Moving Data Files Between Disk Groups With ALTER DATABASE	5-10

Oracle Database File Mapping for Oracle ASM Files	5-10
Managing Alias Names for Oracle ASM File Names	5-13
Adding an Alias Name for an Oracle ASM File Name.....	5-13
Renaming an Alias Name for an Oracle ASM File Name	5-13
Dropping an Alias Name for an Oracle ASM File Name	5-14
Dropping Files and Associated Aliases from a Disk Group	5-14
Managing Disk Group Directories	5-14
Creating a Directory	5-15
Renaming a Directory	5-15
Dropping a Directory	5-16
Accessing Oracle ASM Files with the XML DB Virtual Folder	5-16
Inside /sys/asm	5-16
Using DBMS_FILE Transfer Utility for Oracle ASM	5-17
Managing Disk Group Templates	5-18
Template Attributes	5-19
Adding Templates to a Disk Group.....	5-20
Modifying a Disk Group Template.....	5-21
Dropping Templates from a Disk Group.....	5-21
Creating Tablespaces in Oracle ASM: Specifying Attributes with Templates	5-22
6 Using Views to Display Oracle ASM Information	
Views Containing Oracle ASM Disk Group Information.....	6-1
Viewing Oracle ASM File Access Control Information	6-4
Viewing Disk Region Information	6-5
7 Administering Oracle ASM with Oracle Enterprise Manager	
Accessing the Oracle Automatic Storage Management Home Page.....	7-1
Configuring Oracle ASM Initialization Parameters with Oracle Enterprise Manager.....	7-3
Managing Oracle ASM Users with Oracle Enterprise Manager.....	7-4
Managing Disk Groups with Oracle Enterprise Manager.....	7-5
Creating Disk Groups.....	7-6
Adding Disks to Disk Groups	7-8
Bringing Disks Online and Offline	7-9
Dropping Disks from Disk Groups.....	7-11
Dropping Disk Groups	7-13
Monitoring Disk Group Usage	7-14
Mounting and Dismounting Disk Groups	7-14
Administering Advanced Disk Group Properties.....	7-15
Specifying a Power Limit For Disk Online	7-17
Replacing An Existing Disk With a New Disk.....	7-17
Setting and Modifying Content Type for the Disk Group	7-18
Setting and Modifying the Failure Group Repair Time.....	7-18
Running Rebalance on Multiple Disk Groups	7-19

Viewing Rebalance Process Related Data	7-19
Setting and Modifying the Thin Provisioned Disk Group Attribute	7-19
Running the On Demand Scrubbing Process	7-20
Determining Whether Scrubbing Process Is Running	7-20
Managing Oracle ASM File Access Control with Oracle Enterprise Manager	7-20
Managing Directories, Files, and Aliases with Oracle Enterprise Manager	7-21
Managing Disk Group Templates with Oracle Enterprise Manager	7-22
Managing Oracle ASM Filter Driver With Oracle Enterprise Manager	7-23
Discovering ASM Filter Driver Disks	7-24
Provisioning ASM Filter Driver Disks	7-24
Releasing ASM Filter Driver Disks	7-25
Monitoring Oracle ASM Performance With Oracle Enterprise Manager	7-25
Monitoring General Oracle ASM Performance	7-25
Checking Disk Group Integrity	7-26
Backing Up Oracle ASM Files with Oracle Enterprise Manager	7-27
Performing Bad Block Recovery with Oracle Enterprise Manager	7-27
Migrating to Oracle ASM with Oracle Enterprise Manager	7-28
Monitoring Alerts and Incidents With Oracle ASM Support Workbench	7-29
Monitoring Oracle Flex ASM	7-31

8 Performing Oracle ASM Data Migration with RMAN

Overview of Oracle ASM Data Migration	8-1
Purpose of Oracle ASM Data Migration	8-2
Basic Concepts of Oracle ASM Data Migration	8-2
Basic Steps of Data Migration to Oracle ASM Using RMAN	8-2
Preparing to Migrate the Database to Oracle ASM Using RMAN	8-3
Migrating the Database to Oracle ASM Using RMAN	8-5
Migrating a Database from Oracle ASM to Alternative Storage	8-9
Moving Data Files Between Oracle ASM Disk Groups Using RMAN	8-9

9 Managing Oracle ASM With ASMCA

Getting Started With the ASMCA GUI Tool	9-1
Managing Instances and Disk Groups With ASMCA	9-2
Creating Oracle ASM Instances with ASMCA	9-2
Upgrading an Oracle ASM Instance with ASMCA	9-4
Managing Disk Groups with ASMCA	9-5
ASMCA Command-Line Interface	9-8
Running ASMCA Command-Line	9-8
ASMCA Commands for Instances and Disk Groups	9-9

10 Managing Oracle ASM with ASMCMD

About ASMCMD	10-1
Types of ASMCMD Commands	10-1

About Oracle ASM Files, File Names, Directories, and Aliases	10-2
Preparing to Run ASMCMD	10-6
Running ASMCMD in Interactive Mode	10-7
Running ASMCMD in Noninteractive Mode	10-9
Getting Help	10-10
ASMCMD Instance Management Commands	10-11
dsget	10-12
dsset	10-12
lsct	10-13
lsop	10-14
lspwusr	10-14
orapwusr	10-15
pwcopy	10-16
pwcreate	10-16
pwdelete	10-17
pwget	10-18
pwmov	10-19
pwset	10-19
showclustermode	10-20
showclusterstate	10-20
showpatches	10-21
showversion	10-21
shutdown	10-22
spbackup	10-23
spcopy	10-24
spget	10-25
spmov	10-25
spset	10-26
startup	10-27
ASMCMD Oracle ASM Filter Driver Management Commands	10-27
afd_configure	10-28
afd_deconfigure	10-29
afd_dsget	10-29
afd_dsset	10-30
afd_filter	10-30
afd_label	10-31
afd_lsdsk	10-31
afd_scan	10-32
afd_state	10-32
afd_unlabel	10-33
ASMCMD File Management Commands	10-33
amdu_extract	10-34
cd	10-34

cp.....	10-35
du.....	10-36
find.....	10-37
ls.....	10-38
lsof.....	10-40
mkalias.....	10-41
mkdir.....	10-41
pwd.....	10-42
rm.....	10-42
rmalias.....	10-43
ASMCMD Disk Group Management Commands.....	10-44
chdg.....	10-45
chkdg.....	10-46
dropdg.....	10-47
iostat.....	10-47
lsattr.....	10-49
lsdg.....	10-50
lsdsk.....	10-52
lsod.....	10-54
md_backup.....	10-55
md_restore.....	10-56
mkdg.....	10-57
mount.....	10-59
offline.....	10-59
online.....	10-60
rebal.....	10-61
remap.....	10-62
setattr.....	10-62
umount.....	10-63
ASMCMD Template Management Commands.....	10-64
chtpl.....	10-64
lstmpl.....	10-65
mktmpl.....	10-66
rmtmpl.....	10-66
ASMCMD File Access Control Commands.....	10-67
chgrp.....	10-68
chmod.....	10-68
chown.....	10-70
groups.....	10-70
grpmod.....	10-71
lsgrp.....	10-72
lsusr.....	10-72
mkgrp.....	10-73

mkusr	10-74
passwd	10-74
rmgrp.....	10-75
rmusr	10-75
rpusr	10-76

Part III Oracle Automatic Storage Management Cluster File System

11 Introducing Oracle ACFS and Oracle ADVM

Overview of Oracle ACFS	11-1
Understanding Oracle ACFS Concepts	11-4
About Oracle ACFS	11-4
About the Oracle ACFS Mount Model and Namespace	11-5
About Oracle ACFS and Database Data Files	11-5
About Oracle ACFS and Oracle Database Homes.....	11-7
About Oracle ASM Dynamic Volume Manager	11-9
About the Oracle ACFS Driver Model	11-9
About the Oracle ACFS Mount Registry	11-9
About Oracle ACFS Snapshots.....	11-10
About Oracle ACFS and Backup and Restore.....	11-12
About Oracle ACFS Integration with Oracle ASM	11-12
About Oracle ACFS and External Tables on Windows.....	11-13
Understanding Oracle ACFS Administration	11-13
Oracle ACFS and File Access and Administration Security	11-13
Oracle ACFS and Grid Infrastructure Installation	11-14
Oracle ACFS Configuration.....	11-14
Oracle Clusterware Resources and Oracle ACFS Administration.....	11-14
Oracle ACFS and Dismount or Shutdown Operations.....	11-19
Oracle ACFS Security.....	11-19
Oracle ACFS Encryption	11-22
Oracle ACFS Auditing.....	11-24
Oracle ACFS Replication.....	11-30
Oracle ACFS Tagging	11-33
Using Replication with Auditing, Encryption, and Security	11-35
Oracle ACFS Plugins.....	11-36
High Availability Network File Storage for Oracle Grid Infrastructure.....	11-36
Overview of Oracle ASM Dynamic Volume Manager.....	11-39

12 Using Views to Display Oracle ACFS Information

Views Containing Oracle ACFS Information	12-1
Oracle ACFS Support for Oracle Database File Mapping Views	12-6

13 Administering Oracle ACFS with Oracle Enterprise Manager

Managing Oracle ACFS File Systems and Volumes with Oracle Enterprise Manager	13-1
Creating Oracle ACFS File Systems and Volumes	13-2
Viewing and Modifying Oracle ACFS Volumes and File Systems	13-3
Managing Oracle ACFS Snapshots with Oracle Enterprise Manager	13-5
Creating, Modifying, and Viewing Snapshots	13-5
Converting Snapshots Between Read-Only and Read-Write	13-7
Creating Child Snapshots from Existing Snapshots.....	13-7
Managing Security Features with Oracle Enterprise Manager	13-8
Initializing Oracle ACFS Security	13-9
Preparing an Oracle ACFS For Security.....	13-10
Undoing Oracle ACFS Security	13-10
Enabling Security on Oracle ACFS	13-10
Disabling Security on Oracle ACFS	13-11
Viewing Security Status.....	13-11
Adding an Oracle ACFS Security Administrator	13-11
Changing an Oracle ACFS Security Administrator Password	13-11
Deleting an Oracle ACFS Security Administrator.....	13-12
Viewing Oracle ACFS Security Administrators	13-12
Creating a Rule	13-12
Cloning a Rule.....	13-13
Editing a Rule.....	13-13
Deleting a Rule.....	13-14
Searching For and Viewing Rules.....	13-14
Creating a Ruleset	13-15
Cloning a Ruleset.....	13-15
Editing a Ruleset.....	13-16
Deleting a Ruleset.....	13-16
Searching For and Viewing Rulesets	13-17
Creating a Realm	13-18
Cloning a Realm	13-18
Adding Objects to a Realm	13-18
Deleting Objects from a Realm.....	13-19
Deleting a Realm.....	13-19
Viewing Realms.....	13-20
Managing Encryption Features with Oracle Enterprise Manager.....	13-21
Initializing Oracle ACFS Encryption.....	13-21
Enabling, Disabling, and Setting Parameters for Encryption On an Oracle ACFS	13-22
Viewing Encryption Status	13-22
Managing Tagging Features with Oracle Enterprise Manager.....	13-22
Adding a Tag in Oracle ACFS	13-23
Removing a Tag in Oracle ACFS.....	13-23

Searching for Tags in Oracle ACFS.....	13-24
14 Managing Oracle ACFS and Oracle ADVM With ASMCA	
ASMCA GUI Tool for Managing Oracle ACFS and Oracle ADVM.....	14-1
Managing Oracle ADVM Volumes with ASMCA.....	14-1
Managing Oracle ACFS File Systems with ASMCA	14-3
Managing Security and Encryption for Oracle ACFS with ASMCA	14-5
Creating an Oracle ACFS File System for Database Use	14-7
ASMCA Command-Line Interface for Managing Oracle ACFS and Oracle ADVM.....	14-9
ASMCA Commands for Oracle ACFS and Oracle ADVM	14-9
15 Managing Oracle ADVM with ASMCMD	
ASMCMD Volume Management Commands.....	15-1
volcreate	15-1
voldelete.....	15-3
voldisable.....	15-4
volenable.....	15-5
volinfo	15-5
volresize	15-6
volset	15-7
volstat	15-8
16 Managing Oracle ACFS with Command-Line Tools	
Basic Steps to Manage Oracle ACFS Systems.....	16-1
Creating an Oracle ACFS File System	16-2
Accessing an Oracle ACFS File System on a Different Node in the Cluster	16-4
Managing Oracle ACFS Snapshots	16-5
Securing Oracle ACFS File Systems.....	16-6
Encrypting Oracle ACFS File Systems	16-11
Tagging Oracle ACFS File Systems	16-12
Replicating Oracle ACFS File Systems	16-13
Deregistering, Dismounting, and Disabling Volumes and Oracle ACFS File Systems	16-19
Removing an Oracle ACFS File System and a Volume	16-21
Oracle ACFS Command-line Tools for Linux Environments	16-21
fsck.....	16-22
mkfs	16-24
mount	16-26
umount.....	16-27
Oracle ACFS Command-line Tools for the Solaris Environment	16-28
fsck.....	16-29
mkfs	16-30
mount	16-32
umount/umountall.....	16-33

Oracle ACFS Command-line Tools for the AIX Environment.....	16-34
fsck.....	16-35
mkfs.....	16-37
mount.....	16-38
umount/umountall.....	16-40
Oracle ACFS Command-line Tools for Windows Environments.....	16-41
acfschkdisk.....	16-41
acfsdismount.....	16-43
acfsformat.....	16-44
acfsmountvol.....	16-45
acfsutil detach.....	16-46
advmutil dismount.....	16-47
advmutil list.....	16-48
advmutil mount.....	16-49
Oracle ACFS Command-Line Tools for Tagging.....	16-50
acfsutil tag info.....	16-50
acfsutil tag set.....	16-51
acfsutil tag unset.....	16-53
Oracle ACFS Command-Line Tools for Replication.....	16-53
acfsutil repl bg.....	16-54
acfsutil repl compare.....	16-55
acfsutil repl info.....	16-56
acfsutil repl init.....	16-58
acfsutil repl pause.....	16-60
acfsutil repl resume.....	16-61
acfsutil repl sync.....	16-62
acfsutil repl terminate.....	16-63
acfsutil repl trace.....	16-64
acfsutil repl update.....	16-64
Oracle ACFS Command-Line Tools for Auditing.....	16-65
acfsutil audit archive.....	16-66
acfsutil audit disable.....	16-67
acfsutil audit enable.....	16-67
acfsutil audit info.....	16-68
acfsutil audit init.....	16-68
acfsutil audit purge.....	16-69
acfsutil audit read.....	16-70
Oracle ACFS Command-Line Tools for Security.....	16-70
acfsutil sec admin add.....	16-72
acfsutil sec admin password.....	16-73
acfsutil sec admin remove.....	16-73
acfsutil sec batch.....	16-74
acfsutil sec disable.....	16-74

acfsutil sec enable	16-75
acfsutil sec info.....	16-76
acfsutil sec info file	16-77
acfsutil sec init.....	16-77
acfsutil sec load.....	16-79
acfsutil sec prepare.....	16-79
acfsutil sec realm add.....	16-82
acfsutil sec realm audit disable.....	16-85
acfsutil sec realm audit enable.....	16-85
acfsutil sec realm audit info	16-87
acfsutil sec realm clone	16-88
acfsutil sec realm create	16-89
acfsutil sec realm delete.....	16-90
acfsutil sec realm destroy	16-91
acfsutil sec rule clone	16-92
acfsutil sec rule create	16-93
acfsutil sec rule destroy	16-94
acfsutil sec rule edit.....	16-95
acfsutil sec ruleset clone	16-95
acfsutil sec ruleset create	16-96
acfsutil sec ruleset destroy	16-97
acfsutil sec ruleset edit.....	16-98
acfsutil sec save.....	16-98
Oracle ACFS Command-Line Tools for Encryption.....	16-99
acfsutil encr info	16-100
acfsutil encr init	16-101
acfsutil encr off.....	16-101
acfsutil encr on.....	16-102
acfsutil encr rekey.....	16-103
acfsutil encr set.....	16-105
acfsutil keystore migrate	16-106
Oracle ACFS Command-Line Utilities	16-107
acfsdbg	16-108
acfsutil info file	16-110
acfsutil info fs	16-111
acfsutil info id	16-115
acfsutil plugin disable.....	16-116
acfsutil plugin enable.....	16-116
acfsutil plugin info	16-118
acfsutil registry	16-119
acfsutil rmfs.....	16-121
acfsutil size	16-122
acfsutil snap convert	16-123

acfsutil snap create	16-124
acfsutil snap delete	16-126
acfsutil snap info.....	16-127
acfsutil tune	16-129
advmutil canonical.....	16-130
advmutil tune.....	16-131
advmutil volinfo.....	16-131

Part IV Additional Information

17 Creating Database Files in Oracle ASM Using SQL*Plus

Creating a Database that Uses Oracle ASM	17-1
Creating Tablespaces in Oracle ASM.....	17-2
Creating Redo Logs in Oracle ASM	17-2
Creating Control Files in Oracle ASM	17-3
Creating Control Files in Oracle ASM: Example 1	17-3
Creating Control Files in Oracle ASM: Example 2	17-4
Creating Archive Log Files in Oracle ASM.....	17-4

18 Understanding Oracle ACFS Advanced Topics

Limits of Oracle ACFS.....	18-1
Oracle ACFS Disk Space Usage.....	18-2
Oracle ACFS Error Handling.....	18-2
Oracle ACFS and NFS.....	18-3
Limits of Oracle ADVM	18-3
Oracle ACFS Drivers Resource Management.....	18-4
Oracle ACFS Registry Resource Management	18-4
Oracle ACFS File System Resource Management.....	18-4
Oracle ACFS and Oracle Restart.....	18-5
Oracle ACFS Driver Commands	18-5
acfsload	18-5
acfsdriverstate	18-6
Oracle ACFS Plug-in Generic Application Programming Interface	18-7
Oracle ACFS Pre-defined Metric Types	18-7
acfsplugin	18-7
Oracle ACFS Tagging Generic Application Programming Interface.....	18-10
Oracle ACFS Tag Name Specifications	18-10
Oracle ACFS Tagging Error Values.....	18-11
acfsgettag	18-11
acfslisttags.....	18-12
acfsremovetag	18-14
acfssettag.....	18-14
Understanding Oracle ACFS I/O Failure Console Messages.....	18-15

Glossary

Index

List of Tables

1	One operating system group and one set of privileges for all Oracle ASM users.....	3-47
2	Separated operating system groups and privileges for Oracle ASM users.....	3-48
1	Mirroring options for Oracle ASM disk group types.....	4-30
2	Examples of disk group compatibility attribute settings.....	4-43
3	Oracle ASM features enabled by disk group compatibility attribute settings.....	4-46
4	Oracle ACFS features enabled by disk group compatibility attribute settings.....	4-47
5	Maximum Oracle ASM file sizes for disk groups with AU_SIZE equal to 1 MB.....	4-48
1	File types supported by Oracle ASM.....	5-1
2	Valid usage for Oracle ASM file name forms.....	5-4
3	Oracle file types and Oracle ASM file type tags.....	5-5
4	Permitted values for Oracle ASM template striping attribute.....	5-19
5	Permitted values for Oracle ASM template redundancy attribute.....	5-19
6	Oracle ASM system default templates attribute settings.....	5-19
7	Permitted values for Oracle ASM template primary and mirror region attribute.....	5-20
1	Oracle ASM dynamic views for disk group information.....	6-1
1	Options for the ASMCA command-line tool.....	9-8
2	Options for the -convertToFlexASM command.....	9-10
3	Options for the -configureASM command.....	9-11
4	Options for the -configureParameter command.....	9-12
5	Options for the -deleteASM command.....	9-13
6	Options for the -createDiskGroup command.....	9-13
7	Options for the -addDisk command.....	9-15
1	Types of ASMCMD commands.....	10-2
2	ASMCMD interactive options.....	10-7
3	ASMCMD return codes.....	10-9
4	Summary of ASMCMD instance management commands.....	10-11
5	Options for the dsget command.....	10-12
6	Options for the dsset command.....	10-13
7	Options for the lsct command.....	10-14
8	Options for the lspwusr command.....	10-15
9	Options for the orapwusr command.....	10-15
10	Options for the pwcopy command.....	10-16
11	Options for the pwcreate command.....	10-17
12	Options for the pwdelete command.....	10-17
13	Options for the pwget command.....	10-18
14	Options for the pwmove command.....	10-19
15	Options for the pwset command.....	10-20
16	Options for the showversion command.....	10-21
17	Options for the shutdown command.....	10-22
18	Options for the spbackup command.....	10-23
19	Options for the spcopy command.....	10-24
20	Options for the spmove command.....	10-26
21	Options for the spset command.....	10-27
22	Options for the startup command.....	10-27
23	Summary of ASMCMD Oracle ASM Filter Driver management commands.....	10-28
24	Options for the afd_dsset command.....	10-30
25	Options for the afd_filter command.....	10-30
26	Options for the afd_label command.....	10-31
27	Options for the afd_scan command.....	10-32
28	Options for the afd_unlabel command.....	10-33
29	Summary of ASMCMD file management commands.....	10-33

30	Options for the amdu_extract command	10-34
31	Options for the cd command	10-34
32	Options for the cp command	10-35
33	Options for the du command.....	10-37
34	Options for the find command	10-37
35	Options for the ls command.....	10-38
36	Options for the lsof command.....	10-40
37	Options for the mkalias command.....	10-41
38	Options for the mkdir command.....	10-41
39	Options for the rm command.....	10-42
40	Options for the rmalias command.....	10-43
41	Summary of ASMCMD Disk group management commands.....	10-44
42	Options for the chdg command	10-45
43	Options for the chkdg command	10-47
44	Options for the dropdg command	10-47
45	Options for the iostat command.....	10-48
46	Attribute descriptions for iostat command output.....	10-48
47	Options for the lsattr command.....	10-49
48	Options for the lsdg command.....	10-51
49	Attribute descriptions for lsdg command output.....	10-51
50	Options for the lsdsk command.....	10-52
51	Options for the lsod command.....	10-54
52	Options for the md_backup command.....	10-55
53	Options for the md_restore command.....	10-56
54	Options for the mkdg command	10-57
55	Options for the mount command	10-59
56	Options for the offline command.....	10-60
57	Options for the online command.....	10-60
58	Options for the rebal command.....	10-61
59	Options for the remap command.....	10-62
60	Options for the setattr command.....	10-63
61	Options for the umount command	10-63
62	Summary of ASMCMD template management commands.....	10-64
63	Options for the chtmpl command	10-64
64	Options for the lstmpl command.....	10-65
65	Options for the mktmpl command	10-66
66	Options for the rmtmpl command	10-67
67	Summary of ASMCMD file access control commands.....	10-67
68	Options for the chgrp command	10-68
69	Options for the chmod command	10-69
70	Options for the chown command	10-70
71	Options for the groups command	10-71
72	Options for the grpmod command	10-71
73	Options for the lsgrp command.....	10-72
74	Options for the lsusr command.....	10-73
75	Options for the mkggrp command	10-73
76	Options for the mkusr command.....	10-74
77	Options for the passwd command.....	10-74
78	Options for the rmgrp command	10-75
79	Options for the rmusr command.....	10-76
80	Options for the rpusr command.....	10-76
1	Oracle ASM dynamic views for Oracle ACFS information.....	12-1
1	Options for the -createVolume command.....	14-10
2	Options for the -createACFS command.....	14-10

1	Summary of ASMCMD volume management commands.....	15-1
2	Options for the volcreate command.....	15-2
3	Options for the voldelete command.....	15-4
4	Options for the voldisable command.....	15-4
5	Options for the volenable command.....	15-5
6	Options for the volinfo command.....	15-6
7	Options for the volresize command.....	15-7
8	Options for the volset command.....	15-7
9	Options for the volstat command.....	15-8
1	Summary of Oracle ACFS commands for Linux environments.....	16-22
2	Options for the Linux fsck command.....	16-22
3	Options for the Linux mkfs command.....	16-24
4	Options for the Linux mount command.....	16-26
5	Options for the Linux umount command.....	16-27
6	Summary of Oracle ACFS commands for Solaris.....	16-28
7	Options for the Solaris fsck command.....	16-29
8	Options for the Solaris mkfs command.....	16-31
9	Options for the Solaris mount command.....	16-32
10	Options for the Solaris umount command.....	16-34
11	Summary of Oracle ACFS commands for AIX.....	16-35
12	Options for the AIX fsck command.....	16-36
13	Options for the AIX mkfs command.....	16-37
14	Options for the AIX mount command.....	16-39
15	Options for the AIX umount command.....	16-40
16	Summary of Oracle ACFS file system commands for Windows.....	16-41
17	Summary of Non-Oracle ACFS file system commands for Windows.....	16-41
18	Options for the acfschkdsk command.....	16-41
19	Options for the acfsdismount command.....	16-43
20	Options for the acfsformat command.....	16-44
21	Options for the acfsmountvol command.....	16-45
22	Options for the advmutil dismount command.....	16-47
23	Options for the advmutil list command.....	16-48
24	Options for the advmutil mount command.....	16-49
25	Summary of commands for Oracle ACFS tagging.....	16-50
26	Options for the acfsutil tag info command.....	16-51
27	Options for the acfsutil tag set command.....	16-52
28	Options for the acfsutil tag unset command.....	16-53
29	Summary of commands for Oracle ACFS replication.....	16-54
30	Options for the acfsutil repl bg command.....	16-55
31	Options for the acfsutil repl compare command.....	16-56
32	Options for the acfsutil repl info command.....	16-57
33	Options for the acfsutil repl init command.....	16-58
34	Options for the acfsutil repl pause command.....	16-61
35	Options for the acfsutil repl resume command.....	16-62
36	Options for the acfsutil repl sync command.....	16-62
37	Options for the acfsutil repl terminate command.....	16-63
38	Options for the acfsutil repl trace command.....	16-64
39	Options for the acfsutil repl update command.....	16-65
40	Summary of commands for Oracle ACFS auditing.....	16-66
41	Options for the acfsutil audit archive command.....	16-66
42	Options for the acfsutil audit disable command.....	16-67
43	Options for the acfsutil audit enable command.....	16-67
44	Options for the acfsutil audit info command.....	16-68
45	Options for the acfsutil audit init command.....	16-69

46	Options for the acfsutil audit purge command.....	16-70
47	Options for the acfsutil audit read command.....	16-70
48	Summary of commands for Oracle ACFS security.....	16-71
49	Options for the acfsutil sec admin add command.....	16-72
50	Options for the acfsutil sec admin remove command.....	16-73
51	Options for the acfsutil sec batch command.....	16-74
52	Options for the acfsutil sec disable command.....	16-75
53	Options for the acfsutil sec enable command.....	16-75
54	Options for the acfsutil sec info command.....	16-76
55	Options for the acfsutil sec info file command.....	16-77
56	Options for the acfsutil sec init command.....	16-78
57	Options for the acfsutil sec load command.....	16-79
58	Options for the acfsutil sec prepare command.....	16-80
59	Options for the acfsutil sec realm add command.....	16-82
60	Command Rules.....	16-83
61	Options for the acfsutil sec realm audit disable command.....	16-85
62	Options for the acfsutil sec realm audit enable command.....	16-86
63	Options for the acfsutil sec realm audit info command.....	16-88
64	Options for the acfsutil sec realm clone command.....	16-88
65	Options for the acfsutil sec realm create command.....	16-89
66	Options for the acfsutil sec realm delete command.....	16-90
67	Options for the acfsutil sec realm destroy command.....	16-92
68	Options for the acfsutil sec rule clone command.....	16-92
69	Options for the acfsutil sec rule create command.....	16-93
70	Options for the acfsutil sec rule destroy command.....	16-94
71	Options for the acfsutil sec rule edit command.....	16-95
72	Options for the acfsutil sec ruleset clone command.....	16-96
73	Options for the acfsutil sec ruleset create command.....	16-97
74	Options for the acfsutil sec ruleset destroy command.....	16-97
75	Options for the acfsutil sec ruleset edit command.....	16-98
76	Options for the acfsutil sec save command.....	16-99
77	Summary of commands for Oracle ACFS encryption.....	16-99
78	Options for the acfsutil encr info command.....	16-100
79	Options for the acfsutil encr init command.....	16-101
80	Options for the acfsutil encr off command.....	16-102
81	Options for the acfsutil encr on command.....	16-103
82	Options for the acfsutil encr rekey command.....	16-104
83	Options for the acfsutil encr set command.....	16-105
84	Options for the acfsutil keystore migrate command.....	16-106
85	Summary of Oracle ACFS command-line utilities.....	16-107
86	Options for the acfsdbg command.....	16-108
87	Subcommands for acfsdbg.....	16-108
88	Options for the acfsutil info file command.....	16-111
89	Options for the acfsutil info fs command.....	16-111
90	Options for the acfsutil info id command.....	16-115
91	Options for the acfsutil plugin disable command.....	16-116
92	Options for the acfsutil plugin enable command.....	16-117
93	Options for the acfsutil plugin info command.....	16-119
94	Options for the acfsutil registry command.....	16-120
95	Options for the acfsutil rmfs command.....	16-122
96	Options for the acfsutil size command.....	16-122
97	Options for the acfsutil snap convert command.....	16-124
98	Options for the acfsutil snap create command.....	16-124
99	Options for the acfsutil snap delete command.....	16-127

100	Options for the acfsutil snap info command.....	16-127
101	Options for the acfsutil tune command.....	16-129
102	Options for the advmutil canonical command.....	16-130
103	Options for the advmutil tune command.....	16-131
104	Options for the advmutil volinfo command.....	16-132
1	Options for the acfsload command.....	18-6
2	Options for the acfsdriverstate command.....	18-6
3	Options for the acfsgettag command.....	18-11
4	Options for the acfslisttags command.....	18-12
5	Options for the acfsremovetag command.....	18-14
6	Options for the acfssettag command.....	18-15

List of Figures

1	Oracle ASM for Single-Instance Oracle Databases	1-4
2	Oracle ASM Cluster Configuration with Oracle RAC.....	1-4
3	Oracle ASM Cluster with Single-Instance Oracle Databases.....	1-5
4	Oracle ASM File Allocation in a Disk Group.....	1-9
5	Oracle ASM Fine-Grained Striping.....	1-10
6	Oracle ASM Coarse-Grained Striping.....	1-10
1	Oracle Flex ASM Configurations.....	3-16
2	Oracle ACFS and Oracle ADVM in Oracle Flex ASM.....	3-18
3	Oracle ASM Configuration Assistant Configure ASM Instances Page.....	3-32
4	Oracle ASM Configuration Assistant Convert to Oracle Flex ASM Dialog Box.....	3-32
5	Oracle ASM Configuration Assistant ASM Conversion Dialog Box.....	3-33
1	Hierarchical Structure of Oracle ASM Folders in an XML DB Installation.....	5-17
1	Oracle Automatic Storage Management Home Page.....	7-2
2	Oracle Automatic Storage Management Configuration Parameters Page.....	7-3
3	Oracle Automatic Storage Management Users Page.....	7-4
4	Oracle Automatic Storage Management Create Disk Group Page.....	7-7
5	Oracle Automatic Storage Management Disk Groups List Page.....	7-10
6	Oracle Automatic Storage Management Disk Group General Page.....	7-10
7	Oracle Automatic Storage Management Edit Advanced Attributes Page.....	7-15
8	Oracle Automatic Storage Management Disk Group Access Control Home Page.....	7-21
9	Oracle Automatic Storage Management Files Tab.....	7-22
10	Oracle Automatic Storage Management Templates Page.....	7-23
11	Oracle Automatic Storage Management Performance Page.....	7-26
12	Oracle Automatic Storage Management Check Diskgroup Confirmation Dialog.....	7-27
13	Oracle Automatic Storage Management Support Workbench Problems.....	7-30
14	Oracle Automatic Storage Management Support Workbench Packages.....	7-31
15	Oracle Flex ASM Home Page.....	7-31
16	Oracle Flex ASM Members Page.....	7-32
17	Oracle Flex ASM Topology Page.....	7-32
1	Oracle ASM Configuration Assistant Create ASM Page.....	9-3
2	Oracle ASM Configuration Assistant Create ASM Page.....	9-4
3	Oracle ASM Configuration Assistant Upgrade ASM Page.....	9-5
4	Oracle ASM Configuration Assistant Configure Disk Groups Page.....	9-6
5	Oracle ASM Configuration Assistant Create Disk Groups Page.....	9-7
6	Oracle ASM Configuration Assistant Create Disk Groups - Advanced Options.....	9-8
1	Oracle Automatic Storage Management Storage Layers.....	11-2
1	Oracle ACFS Create ASM Volume Page.....	13-2
2	Oracle ACFS Page.....	13-4
3	Oracle ACFS General Page.....	13-4
4	Oracle ACFS Volume Page.....	13-5
5	Oracle ACFS Snapshots Tab.....	13-6
6	Oracle ACFS Create Snapshot Page.....	13-7
7	Oracle ACFS Security Configuration Page.....	13-9
8	Oracle ACFS Security Rules Page.....	13-15
9	Oracle ACFS Security Rulesets Page.....	13-17
10	Oracle ACFS Security Realms Page.....	13-21
11	Oracle ACFS Encryption Configuration Page.....	13-22
1	Oracle ASM Configuration Assistant Configure ASM Volumes Page.....	14-2
2	Oracle ASM Configuration Assistant Create an ASM Volume Page.....	14-3
3	Oracle ASM Configuration Assistant Configure Oracle ACFS Page.....	14-4
4	Oracle ASM Configuration Assistant Create Oracle ACFS Dialog.....	14-5

5	Oracle ASM Configuration Assistant Configure Security and Encryption Dialog.....	14-6
6	Oracle ASM Configuration Assistant Oracle ACFS Security Menu Options.....	14-7
7	Oracle ASM Configuration Assistant Create Oracle ACFS for Database Use Dialog.....	14-9

Preface

The *Oracle Automatic Storage Management Administrator's Guide* describes how to administer Oracle Automatic Storage Management (Oracle ASM) for Oracle Database.

This Preface contains the following topics:

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

Audience

The audience for this book includes system administrators, database administrators, and storage administrators. The *Oracle Automatic Storage Management Administrator's Guide* is intended for database and storage administrators who perform the following tasks:

- Administer and manage Oracle ASM
- Configure and administer Oracle ASM

To use this document, you should be familiar with basic Oracle Database concepts and administrative procedures. Also, you might want to review the documentation for Oracle Clusterware and Oracle Real Application Clusters (Oracle RAC). See "[Related Documents](#)".

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

For more information, refer to the following Oracle resources:

- *Oracle Database Administrator's Guide*
- *Oracle Database Concepts*
- *Oracle Database Reference*
- *Oracle Database SQL Language Reference*
- *Oracle Database 2 Day + Real Application Clusters Guide*
- *Oracle Clusterware Administration and Deployment Guide*
- *Oracle Real Application Clusters Administration and Deployment Guide*
- Platform-specific guides, including Oracle Database, Oracle Grid Infrastructure, and Oracle Real Application Clusters installation guides

Conventions

The following text conventions are used in this document:

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

Changes in This Release for Oracle Automatic Storage Management Administrator's Guide

This chapter describes changes in *Oracle Automatic Storage Management Administrator's Guide*.

- [Changes in Oracle Automatic Storage Management 12c Release 1 \(12.1.0.2\)](#)
- [Changes in Oracle Automatic Storage Management 12c Release 1 \(12.1.0.1\)](#)
- [Changes in Oracle ACFS and Oracle ADVM for Oracle ASM 12c Release 1 \(12.1.0.2\)](#)
- [Changes in Oracle ACFS and Oracle ADVM for Oracle ASM 12c Release 1 \(12.1.0.1\)](#)

See Also:

Oracle Database New Features Guide for a complete description of the new features in Oracle Database 12c Release 1 (12.1)

Changes in Oracle Automatic Storage Management 12c Release 1 (12.1.0.2)

This section describes changes to Oracle Automatic Storage Management 12c Release 1 (12.1.0.2).

This section contains the following topic:

- [New Features](#)

New Features

The following are new features for Oracle ASM 12c Release 1 (12.1.0.2):

- [Oracle ASM Filter Driver](#)

Oracle ASM Filter Driver

Note:

This feature is available on Linux systems starting with Oracle Database 12c Release 1 (12.1.0.2).

Oracle ASM Filter Driver (Oracle ASMFDF) is a kernel module that resides in the I/O path of the Oracle ASM disks. Oracle ASM uses the filter driver to validate write I/O requests to Oracle ASM disks.

The Oracle ASM Filter Driver rejects any I/O requests that are invalid. This action eliminates accidental overwrites of Oracle ASM disks that would cause corruption in the disks and files within the disk group. For example, the Oracle ASM Filter Driver filters out all non-Oracle I/Os which could cause accidental overwrites.

For more information about Oracle ASMFDF, refer to “[Oracle ASM Filter Driver](#)”.

Changes in Oracle Automatic Storage Management 12c Release 1 (12.1.0.1)

This section describes changes to Oracle Automatic Storage Management 12c Release 1 (12.1.0.1).

- [New Features](#)
- [Deprecated Features](#)
- [Desupported Features](#)

New Features

The following are new features for Oracle ASM 12c Release 1 (12.1.0.1):

- [General Oracle ASM Enhancements](#)
- [Oracle Flex ASM](#)
- [Oracle ASM Disk Scrubbing](#)
- [Oracle ASM Disk Resync Enhancements](#)
- [Even Read For Disk Groups](#)
- [Oracle ASM Rebalance Enhancements](#)
- [Shared Oracle ASM Password File in a Disk Group](#)
- [Oracle ASM File Access Control Enhancements on Windows](#)
- [Rolling Migration Framework for Oracle ASM One-off Patches](#)
- [Updated Key Management Framework](#)
- [Oracle Enterprise Manager](#)

General Oracle ASM Enhancements

This feature provides general enhancements to Oracle ASM, including:

- Revised version of the physical metadata replication point

Oracle ASM now replicates physically addressed metadata, such as the disk header and allocation tables, within each disk. This enhancement ensures that Oracle ASM is more resilient to bad disk sectors and external corruptions. The disk group attribute `PHYS_META_REPLICATED` is provided to track the replication status of a disk group.

For more information on the `PHYS_META_REPLICATED` attribute, refer to [“PHYS_META_REPLICATED”](#).

- Support for increased storage limits

Oracle ASM now supports 511 disk groups. The maximum Oracle ASM disk size is now 32 petabytes (PB).

For information about Oracle ASM size limits, refer to [“Oracle ASM Storage Limits”](#).

- The `ALTER DISKGROUP` statement has been updated with a `REPLACE` clause.

For more information about replacing disks in a disk group, refer to [“Replacing Disks in Disk Groups”](#).

Oracle Flex ASM

Oracle Flex ASM enables an Oracle ASM instance to run on a separate physical server from the database servers. Many Oracle ASM instances can be clustered to support a large number of database clients.

This feature enables you to consolidate all the storage requirements into a single set of disk groups. All these disk groups can be managed by a small set of Oracle ASM instances running in a single cluster.

Oracle Flex ASM supports only Oracle Database 12c Release 1 (12.1) and later releases.

For information, refer to [“Managing Oracle Flex ASM”](#).

Oracle ASM Disk Scrubbing

Oracle ASM disk scrubbing checks logical data corruptions and repairs the corruptions automatically in normal and high redundancy disks groups. The feature is designed so that it does not have any impact to the regular input and output (I/O) operations in production systems. The scrubbing process repairs logical corruptions using the Oracle ASM mirror disks. Disk scrubbing uses Oracle ASM rebalancing to minimize I/O overhead.

The scrubbing process is visible in fields of the `V$ASM_OPERATION` view.

For more information, refer to [“Scrubbing Disk Groups”](#).

Oracle ASM Disk Resync Enhancements

The disk resync enhancements enable fast recovery from instance failure and faster resync performance overall. Oracle ASM disk resync enables multiple disks to be brought online simultaneously or to control the speed of the resync operation. Oracle ASM disk resync has a resync power limit to control resync parallelism and improve performance. Disk resync checkpoint functionality provides faster recovery from

instance failures by enabling the resync to resume from the point at which the process was interrupted or stopped, instead of starting from the beginning.

For more information about disk resync, refer to [“Oracle ASM Fast Mirror Resync”](#).

Even Read For Disk Groups

The even read feature distributes data reads evenly across all the disks in a disk group. For each I/O request presented to the system, there may be one or more disks that contain the data. With this feature, each request to read can be sent to the least loaded of the possible source disks.

Even read functionality is enabled by default on all Oracle Database and Oracle ASM instances of version 12.1 and higher in non-Exadata environments. The functionality is enabled in an Exadata environment when there is a failure. Even read functionality is applicable only to disk groups with normal or high redundancy.

For information about even read for disk groups, refer to [“Even Read for Disk Groups”](#).

Oracle ASM Rebalance Enhancements

Oracle ASM rebalance enhancements improve scalability, performance, and reliability of the rebalance operation. This feature extends the rebalance process to operate on multiple disk groups in a single instance. In addition, this feature improves support for thin provisioning, user-data validation, and improved error handling.

For more information about disk group rebalancing, refer to [“Manually Rebalancing Disk Groups”](#) and [“Tuning Rebalance Operations”](#).

Shared Oracle ASM Password File in a Disk Group

This feature implements the infrastructure needed to address the bootstrapping issues of Oracle ASM shared password file in an Oracle ASM disk group. This feature solves the bootstrapping problem for storing shared Oracle ASM password files in a disk group.

For information about a shared password file in a disk group, refer to [“Managing a Shared Password File in a Disk Group”](#). For information about ASMCMD commands to manage an Oracle ASM or database instance password file in a disk group, refer to [“ASMCMD Instance Management Commands”](#).

See Also:

- *Oracle Database Administrator's Guide* for information about ORAPWD commands
 - *Oracle Database Administrator's Guide* for information SRVCTL commands
 - *Oracle Real Application Clusters Administration and Deployment Guide* for information about SRVCTL commands
-
-

Oracle ASM File Access Control Enhancements on Windows

This feature provides enhancements to Oracle ASM File Access Control on Windows platforms.

Oracle Database now supports the use of an Oracle home user, which can be specified at installation time. The Oracle home user is associated with an Oracle home and it cannot be changed after installation. Different Oracle homes on a system can share the same Oracle home user or use different Oracle home user names. For more information, refer to “[About Oracle Home User on Windows](#)”.

You can now use access control to separate roles in Windows environments. With Oracle Database services running as users rather than Local System, the Oracle ASM access control feature is enabled to support role separation on Windows. In previous releases, this feature was disabled on Windows because all Oracle services run as Local System.

You can change the identity of an Oracle ASM user from one operating system (OS) user to another OS user without having to drop and re-create the user, which requires dropping all the files a user owns, which improves the manageability of Oracle ASM users and the files they own.

You can modify Windows file access controls while files are open using ASMCMD file access control commands, such as `chgrp`, `chmod`, and `chown`.

For more information about Oracle ASM File Access Control, refer to “[Managing Oracle ASM File Access Control for Disk Groups](#)”. For information about Oracle ASM File Access Control ASMCMD commands, refer to “[ASMCMD File Access Control Commands](#)”.

See Also:

Oracle Database Platform Guide for Microsoft Windows for information about running Oracle services on Windows platforms, different types of Windows user accounts, and access control on Windows platforms

Rolling Migration Framework for Oracle ASM One-off Patches

This feature enhances the rolling migration framework to apply oneoff patches released for Oracle ASM in a rolling manner.

You can use this feature in a clustered Oracle ASM 12c Release 1 (12.1) and higher environment to update one node at a time to the latest patch level without affecting the overall availability of the Oracle ASM cluster or the database clusters using Oracle ASM for storage. This feature improves database availability by migrating the database to another Oracle ASM instance before a shut down and upgrade operation.

For information, refer to “[About Oracle ASM Rolling Patches](#)”.

See Also:

Oracle Grid Infrastructure Installation Guide for information about rolling migration of Oracle ASM and Oracle Grid Infrastructure homes

Updated Key Management Framework

This feature updates Oracle key management commands to unify the key management application programming interface (API) layer. The updated key management framework makes interacting with keys in the wallet easier and adds new key metadata that describes how the keys are being used.

This feature adds a new capability to store a credential file (wallet) in Oracle ASM disk groups. For information about file types supported by Oracle ASM, refer to “[What Types of Files Does Oracle ASM Support?](#)”.

See Also:

Oracle Database Advanced Security Guide for information about the Oracle key management framework

Oracle Enterprise Manager

Oracle Enterprise Manager replaces Enterprise Manager Database Control for administering Oracle Automatic Storage Management. For more information, refer to [Administering Oracle ASM with Oracle Enterprise Manager](#).

Deprecated Features

The following are the Oracle ASM 12c Release 1 (12.1.0.1) deprecated features.

Deprecation of single letter SRVCTL CLI options in future releases

All SRVCTL commands have been enhanced to accept more meaningful and user-friendly keyword-style options instead of the single letter options. All new SRVCTL command line interface options added in this release support keyword-style options only and do not have single-letter equivalents. The previous style of using single-letter keyword options as existed in previous releases remain fully supported. In a future release, the single-letter options may no longer be supported and customers may want to change their scripts to adapt the keyword-style command options.

Deprecation Announcement for Oracle Restart

Oracle Restart is a feature provided as part of Oracle Grid Infrastructure. Oracle Restart monitors and can restart Oracle Database instances, Oracle Net Listeners, and Oracle ASM instances. Oracle Restart is currently restricted to manage single instance Oracle Databases and Oracle ASM instances only, and is subject to desupport in future releases. Oracle continues to provide Oracle ASM as part of the Oracle Grid Infrastructure installation for Standalone and Cluster deployments.

For more information about the Oracle Restart deprecation announcement and its replacement, see My Oracle Support Note Doc ID 1584742.1 (<https://support.oracle.com/epmos/faces/DocumentDisplay?id=1584742.1&displayIndex=1>).

Desupported Features

The following are the Oracle ASM 12c Release 1 (12.1.0.1) desupported features.

Desupport of RAW (Block) Storage Devices for Oracle Database and Related Technologies

Oracle Database 12c and related technologies, such as Oracle Clusterware 12c, no longer support the use of raw (block) storage devices. This means that files must be moved to Oracle ASM before upgrading to Oracle Clusterware 12c.

Changes in Oracle ACFS and Oracle ADVM for Oracle ASM 12c Release 1 (12.1.0.2)

This section describes changes to Oracle Automatic Storage Management Cluster File System (Oracle ACFS) and Oracle ASM Dynamic Volume Manager (Oracle ADVM) for Oracle ASM 12c Release 1 (12.1.0.2).

This section contains the following topic:

- [New Features](#)

New Features

The following are Oracle ACFS and Oracle ADVM new features in Oracle ASM 12c Release 1 (12.1.0.2):

- [Oracle ACFS Support For Database Data Files on Windows](#)
- [Oracle Exadata Support for Oracle ACFS and Oracle ACFS Support for General Purpose Files](#)
- [Oracle ACFS Support for 1023 Snapshots](#)
- [Oracle ACFS Support for Oracle Database File Mapping Views](#)
- [Oracle ACFS Encryption Support for Oracle Key Vault](#)

Oracle ACFS Support For Database Data Files on Windows

Note:

This feature is available starting with Oracle Database 12c Release 1 (12.1.0.2).

Oracle ACFS in Oracle Grid 12c Release 1 (12.1.0.2) on Windows supports all database files, except for data files and redo logs in an Oracle Restart (standalone server) configuration. For support of database files on Windows, the `COMPATIBLE .ADVM` attribute must be set to `12.1.0.2`.

For more information about database files on Oracle ACFS, refer to “[About Oracle ACFS and Database Data Files](#)”.

Oracle Exadata Support for Oracle ACFS and Oracle ACFS Support for General Purpose Files

Note:

This feature is available starting with Oracle Database 12c Release 1 (12.1.0.2).

Oracle Exadata on Linux supports Oracle ACFS in Oracle Grid 12c Release 1 (12.1.0.2). Oracle ACFS supports general purpose files as well as database files; however, Oracle ASM is the best practice for support of database files.

Oracle ACFS can be configured for use with the database, particularly to leverage Oracle ACFS snapshots for database testing and development. However, Oracle ACFS does not currently have the ability to push database operations directly into storage.

For more information about database files on Oracle ACFS, refer to “[About Oracle ACFS and Database Data Files](#)”.

Oracle ACFS Support for 1023 Snapshots

Note:

This feature is available starting with Oracle Database 12c Release 1 (12.1.0.2).

A total of 1023 read-only, read-write, or combination of read-only and read-write snapshot views are supported for each file system. For information about Oracle ACFS snapshots, refer to “[About Oracle ACFS Snapshots](#)”.

Oracle ACFS Support for Oracle Database File Mapping Views

Note:

This feature is available starting with Oracle Database 12c Release 1 (12.1.0.2).

Oracle ACFS supports Oracle Database file mapping views to the Oracle ASM device level. For information about file mapping views related to Oracle ACFS, refer to “[Oracle ACFS Support for Oracle Database File Mapping Views](#)”.

Oracle ACFS Encryption Support for Oracle Key Vault

Note:

This feature is available starting with Oracle Database 12c Release 1 (12.1.0.2).

Oracle ACFS encryption supports Oracle Key Vault as a key store. For information about using this feature with Oracle ACFS encryption, refer to “[Oracle ACFS Encryption](#)”.

See Also:

Oracle Key Vault Administrator's Guide for information about Oracle Key Vault

Changes in Oracle ACFS and Oracle ADVM for Oracle ASM 12c Release 1 (12.1.0.1)

This section describes changes to Oracle Automatic Storage Management Cluster File System (Oracle ACFS) and Oracle ASM Dynamic Volume Manager (Oracle ADVM) for Oracle ASM 12c Release 1 (12.1.0.1).

This section contains the following topic:

- [New Features](#)

New Features

The following are Oracle ACFS and Oracle ADVM new features in Oracle ASM 12c Release 1 (12.1.0.1):

- [Oracle ACFS Enhancements](#)
- [Oracle ACFS Enhancements Supporting Network File Storage \(NFS\)](#)
- [Enhancements for Oracle ACFS Snapshots](#)
- [Oracle ACFS Tagging Generic Application Programming Interface](#)
- [Oracle Clusterware Resources Supporting Oracle ACFS](#)
- [Oracle ACFS Plugins](#)
- [Integration of Oracle ACFS Replication With Auditing_ Encryption_ and Security](#)
- [Oracle ACFS Auditing and Support for Importing Auditing Data into Audit Vault Server](#)
- [Support for Oracle ACFS Replication and Tagging on Solaris](#)
- [Support for Oracle ACFS Replication and Tagging on AIX](#)
- [Support for Oracle ACFS Security and Encryption on Solaris](#)
- [Oracle Enterprise Manager](#)

Oracle ACFS Enhancements

This feature introduces enhancements for Oracle ACFS, including:

- Oracle ACFS in Oracle Grid 12c Release 1 (12.1) supports all database files for Oracle Database 11g Release 2 (11.2.0.4) or later, except for data files and redo logs in an Oracle Restart (standalone server) configuration. For this feature, the `COMPATIBLE .ADVM` attribute must be set to 12.1 or later for the disk group that contains the Oracle ACFS file system.

Using Oracle ACFS replication or encryption with database files on Oracle ACFS is not supported. For information about other replication options for database files on Oracle ACFS, refer to *Oracle Data Guard Concepts and Administration* and Oracle GoldenGate documentation. Oracle GoldenGate is an Oracle product sold independently of the Oracle Database. To encrypt database data files on Oracle ACFS, Oracle recommends Oracle Advanced Security. Oracle Advanced Security provides Transparent Data Encryption (TDE) to encrypt data files for entire tablespaces. For information about Transparent Data Encryption (TDE), refer to *Oracle Database Advanced Security Guide*.

- Oracle ACFS supports clusterwide, file granular `fcntl` advisory file locking while byte range locks continue to operate in node local mode.
- Oracle ACFS directory listing performance is improved for newly created directories.
- Oracle ACFS supports end-to-end storage visibility for files with the `-d` option of `acfsutil info file`. The `-d` option displays details about a file extent location,

from the Oracle ACFS extent to the Oracle ASM devices in the disk group. For information, refer to [“acfsutil info file”](#).

- Oracle ACFS ASMCMD commands have enhanced syntax. For information about ASMCMD commands for Oracle ACFS, refer to [“ASMCMD Volume Management Commands”](#).
- Oracle ACFS supports unlimited expansions when resizing a file system in a disk group with ADVN compatibility set to 11.2.0.4 or higher.
- Oracle ACFS performance and scalability improvements for `ls` and `find` in a disk group with ADVN compatibility set to 11.2.0.4 or higher.

For more information about Oracle ACFS, refer to [“Overview of Oracle ACFS”](#)

Oracle ACFS Enhancements Supporting Network File Storage (NFS)

Note:

This feature is not supported in Oracle Restart configurations.

High Availability NFS for Oracle Grid Infrastructure provides uninterrupted service of NFS V2/V3/V4 exported paths by exposing NFS exports on Highly Available Virtual IPs (HAVIP) and using Oracle Clusterware agents to ensure that the HAVIPs and NFS exports are always online. While base NFS supports file locking, HANFS does not support NFS file locking.

Oracle ACFS file system exports (using NFS) include Golden Images and patch updates applied to Oracle ACFS snapshots. Note that NFS is deployed with Oracle Grid Infrastructure servers in support of Oracle Grid Infrastructure client systems. Application VIP and NFS export resources are employed for Oracle ACFS and highly available NFS.

High Availability NFS can also be used as a general high availability solution for Oracle ACFS exported file systems.

For information about High Availability NFS for Oracle Grid Infrastructure homes, refer to [“High Availability Network File Storage for Oracle Grid Infrastructure”](#).

See Also:

- *Oracle Real Application Clusters Administration and Deployment Guide* for information about SRVCTL commands
 - *Oracle Clusterware Administration and Deployment Guide* for information about Oracle Clusterware and clusters
-
-

Enhancements for Oracle ACFS Snapshots

Oracle ACFS supports the creation of a snapshot from an existing snapshot in the same Oracle ACFS file system. In addition, snapshot conversions are enabled between read-only and read-write snapshots.

For information about Oracle ACFS snapshots, refer to [“About Oracle ACFS Snapshots”](#). For information about Oracle ACFS snapshot commands, refer to [“Oracle ACFS Command-Line Utilities”](#).

Oracle ACFS Tagging Generic Application Programming Interface

Tagging operations are available as C application programming interfaces (APIs), described in [“Oracle ACFS Tagging Generic Application Programming Interface”](#).

For information about Oracle ACFS tagging, refer to [“Oracle ACFS Tagging”](#). For information about Oracle ACFS tagging operations available through the `acfsutil tag` commands, refer to [“Oracle ACFS Command-Line Tools for Tagging”](#).

Oracle Clusterware Resources Supporting Oracle ACFS

Note:

This feature is not supported in Oracle Restart configurations.

Oracle ACFS and Oracle ADVM resource support is enhanced for both performance and coverage. Oracle Clusterware (CRS) managed resource support is extended to include enhancements for Oracle ACFS Oracle homes, Oracle ACFS General Purpose file systems, and Oracle ADVM volumes in supporting Oracle Grid Infrastructure Server Oracle ACFS export (using NFS) configurations. SRVCTL has updates to commands for managing Oracle ACFS and Oracle ADVM resources.

For information about Oracle Clusterware resources and Oracle ACFS, refer to [“Oracle Clusterware Resources and Oracle ACFS Administration”](#).

See Also:

- *Oracle Real Application Clusters Administration and Deployment Guide* for information about SRVCTL commands
 - *Oracle Clusterware Administration and Deployment Guide* for information about Oracle Clusterware resources
-
-

Oracle ACFS Plugins

The Oracle ACFS plugin functionality enables a user space application to collect *just-in-time* Oracle ACFS file and Oracle ADVM volume metrics from the operating system environment. Applications can use the Oracle ACFS plug-in infrastructure to create customized solutions that extend the general application file metric interfaces to include detailed Oracle ACFS file system and volume data.

For information about Oracle ACFS plugins, refer to [“Oracle ACFS Plugins”](#). For information about Oracle ACFS plugin commands, refer to [“Oracle ACFS Command-Line Utilities”](#). For information about the Oracle ACFS plug-in application programming interface, refer to [“Oracle ACFS Plug-in Generic Application Programming Interface”](#).

Integration of Oracle ACFS Replication With Auditing, Encryption, and Security

This feature enables the integration of Oracle Automatic Storage Management Cluster File System (Oracle ACFS) replication with Oracle ACFS auditing, encryption, and security.

For more information, refer to [“Using Replication with Auditing_ Encryption_ and Security”](#).

Oracle ACFS Auditing and Support for Importing Auditing Data into Audit Vault Server

This feature provides auditing for Oracle ACFS security and encryption. In addition, this feature also generates an XML file containing Oracle ACFS audit trail data which can be imported by Audit Vault Server.

For more information, refer to [“Oracle ACFS Auditing”](#). For information about Oracle ACFS commands for auditing, refer to [“Oracle ACFS Command-Line Tools for Auditing”](#) and the `acfsutil sec realm enable` and `acfsutil sec realm disable` commands described in [“Oracle ACFS Command-Line Tools for Security”](#).

Support for Oracle ACFS Replication and Tagging on Solaris

This feature supports Oracle ACFS replication and tagging on Solaris platforms.

For information about Oracle ACFS, refer to [Introducing Oracle ACFS and Oracle ADVM](#).

Support for Oracle ACFS Replication and Tagging on AIX

This feature supports Oracle ACFS replication and tagging on AIX platforms.

For information about Oracle ACFS, refer to [Introducing Oracle ACFS and Oracle ADVM](#).

Support for Oracle ACFS Security and Encryption on Solaris

This feature extends support for Oracle ACFS Security and Encryption Features on Solaris systems. Changes in functionality for Solaris environments are noted with the individual security and encryption commands.

For more information, refer to [“Oracle ACFS Security”](#) and [“Oracle ACFS Encryption”](#).

Oracle Enterprise Manager

Oracle Enterprise Manager replaces Enterprise Manager Database Control for administering Oracle Automatic Storage Management Cluster File System. For more information, refer to [Administering Oracle ACFS with Oracle Enterprise Manager](#).

Part I

Introduction

Part I provides an overview of Oracle Automatic Storage Management (Oracle ASM) concepts and features in the following chapters:

- [Introducing Oracle Automatic Storage Management](#)
- [Exploring Considerations for Oracle ASM Storage](#)

Introducing Oracle Automatic Storage Management

This chapter describes Oracle Automatic Storage Management (Oracle ASM) concepts and provides an overview of Oracle ASM features. This chapter contains the following topics:

- [Overview of Oracle Automatic Storage Management](#)
- [About Oracle Automatic Storage Management Cluster File System](#)
- [Understanding Oracle ASM Concepts](#)
- [Understanding Oracle ASM Disk Group Administration](#)

For a list of the terms that are used in the *Oracle Automatic Storage Management Administrator's Guide* and their definitions, refer to the [Glossary](#) in this guide.

See Also:

- The Oracle Cloud Storage page on the Oracle Technology Network website at <http://www.oracle.com/technetwork/database/cloud-storage/index.html> for more information about Oracle ASM
 - "Master Note for Automatic Storage Management (ASM) (Doc ID 1187723.1)" at [My Oracle Support \(https://support.oracle.com\)](https://support.oracle.com)
-

Overview of Oracle Automatic Storage Management

Oracle ASM is a [volume manager](#) and a [file system](#) for Oracle Database files that supports single-instance Oracle Database and Oracle Real Application Clusters (Oracle RAC) configurations. Oracle ASM is Oracle's recommended storage management solution that provides an alternative to conventional volume managers, file systems, and raw devices.

Oracle ASM uses [disk groups](#) to store data files; an Oracle ASM disk group is a collection of disks that Oracle ASM manages as a unit. Within a disk group, Oracle ASM exposes a file system interface for Oracle Database files. The content of files that are stored in a disk group is evenly distributed to eliminate hot spots and to provide uniform performance across the disks. The performance is comparable to the performance of raw devices.

You can add or remove disks from a disk group while a database continues to access files from the disk group. When you add or remove disks from a disk group, Oracle ASM automatically redistributes the file contents and eliminates the need for

downtime when redistributing the content. For information about administering disk groups, see [Administering Oracle ASM Disk Groups](#).

The Oracle ASM volume manager functionality provides flexible server-based mirroring options. The Oracle ASM normal and high redundancy disk groups enable two-way and three-way mirroring respectively. You can use external redundancy to enable a Redundant Array of Independent Disks (RAID) storage subsystem to perform the mirroring protection function.

Oracle ASM also uses the Oracle Managed Files (OMF) feature to simplify database file management. OMF automatically creates files in designated locations. OMF also names files and removes them while relinquishing space when tablespaces or files are deleted.

Oracle ASM reduces the administrative overhead for managing database storage by consolidating data storage into a small number of disk groups. The smaller number of disk groups consolidates the storage for multiple databases and provides for improved I/O performance.

Oracle ASM files can coexist with other storage management options such as raw disks and third-party file systems. This capability simplifies the integration of Oracle ASM into pre-existing environments.

Oracle ASM has easy to use management interfaces such as SQL*Plus, the Oracle ASM Command Line Utility (ASMCMD) command-line interface, and Oracle ASM Configuration Assistant (ASMCA). For information about Oracle ASM Configuration Assistant, see [Managing Oracle ASM With ASMCA](#) . For information about the ASMCMD command-line interface, see [Managing Oracle ASM with ASMCMD](#) .

See Also:

Oracle Database Administrator's Guide for information about Oracle Database structure and storage

About Oracle Automatic Storage Management Cluster File System

Oracle Automatic Storage Management Cluster File System (Oracle ACFS) is a multi-platform, scalable file system, and storage management technology that extends Oracle Automatic Storage Management (Oracle ASM) functionality to support all customer files. The Oracle ASM Dynamic Volume Manager (Oracle ADVM) provides volume management services and a standard disk device driver interface to clients.

For more information about Oracle ACFS and Oracle ADVM, refer to [Oracle Automatic Storage Management Cluster File System](#) .

Understanding Oracle ASM Concepts

This section describes concepts for the key Oracle ASM components and it contains the following topics:

- [About Oracle ASM Instances](#)
- [About Oracle ASM Disk Groups](#)
- [About Mirroring and Failure Groups](#)
- [About Oracle ASM Disks](#)

- [About Oracle ASM Allocation Units](#)
- [About Oracle ASM Files](#)

For information about preparing your storage environment, see [Exploring Considerations for Oracle ASM Storage](#).

About Oracle ASM Instances

An Oracle ASM instance is built on the same technology as an Oracle Database instance. An Oracle ASM instance has a System Global Area (SGA) and background processes that are similar to those of Oracle Database. However, because Oracle ASM performs fewer tasks than a database, an Oracle ASM SGA is much smaller than a database SGA. In addition, Oracle ASM has a minimal performance effect on a server. Oracle ASM instances mount disk groups to make Oracle ASM files available to database instances; Oracle ASM instances do not mount databases. For information about managing an Oracle ASM instance, see [Administering Oracle ASM Instances](#).

Oracle ASM is installed in the Oracle Grid Infrastructure home before Oracle Database is installed in a separate Oracle home. Oracle ASM and database instances require shared access to the disks in a disk group. Oracle ASM instances manage the metadata of the disk group and provide file layout information to the database instances.

Oracle ASM metadata is the information that Oracle ASM uses to control a disk group and the metadata resides within the disk group. Oracle ASM metadata includes the following information:

- The disks that belong to a disk group
- The amount of space that is available in a disk group
- The file names of the files in a disk group
- The location of disk group data file [extents](#)
- A redo log that records information about atomically changing metadata blocks
- Oracle ADVM volume information

Oracle ASM instances can be clustered using Oracle Clusterware; there is one Oracle ASM instance for each cluster node. If there are several database instances for different databases on the same node, then the database instances share the same single Oracle ASM instance on that node.

If the Oracle ASM instance on a node in a Standard Oracle ASM cluster fails, then all of the database instances on that node also fail. However, in an Oracle Flex ASM configuration, Oracle 12c database instances would not fail as they would be able to access another Oracle ASM instance remotely on another node. For information about Oracle Flex ASM, refer to "[Managing Oracle Flex ASM](#)".

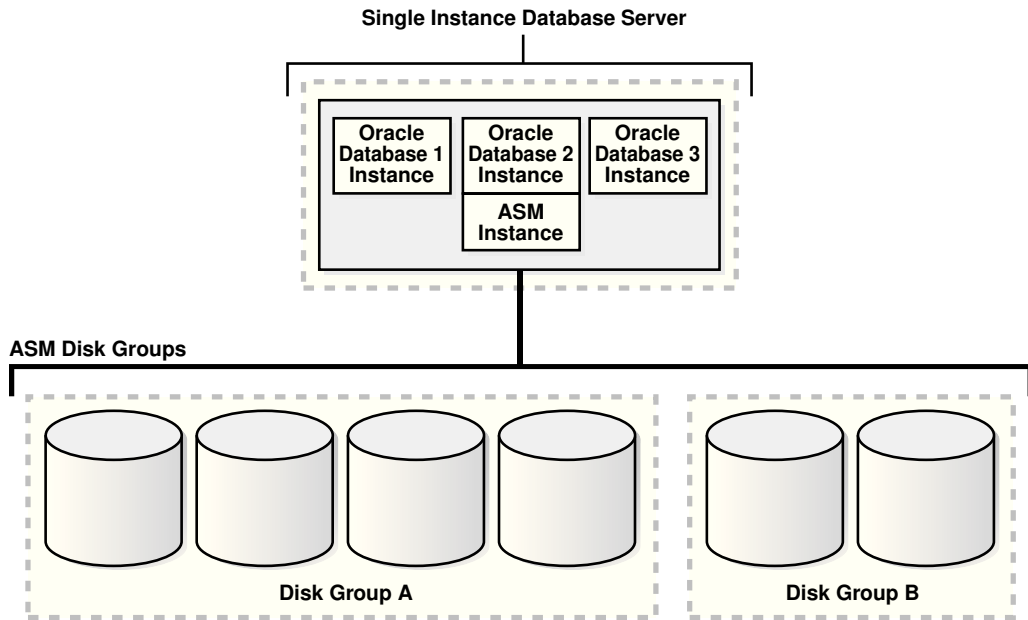
Unlike a file system driver failure, an Oracle ASM instance failure does not require restarting the operating system. In an Oracle RAC environment, the Oracle ASM and database instances on the surviving nodes automatically recover from an Oracle ASM instance failure on a node.

[Figure 1](#) shows a single node configuration with one Oracle ASM instance and multiple database instances. The Oracle ASM instance manages the metadata and provides space allocation for the Oracle ASM files. When a database instance creates or opens an Oracle ASM file, it communicates those requests to the Oracle ASM

instance. In response, the Oracle ASM instance provides file extent map information to the database instance.

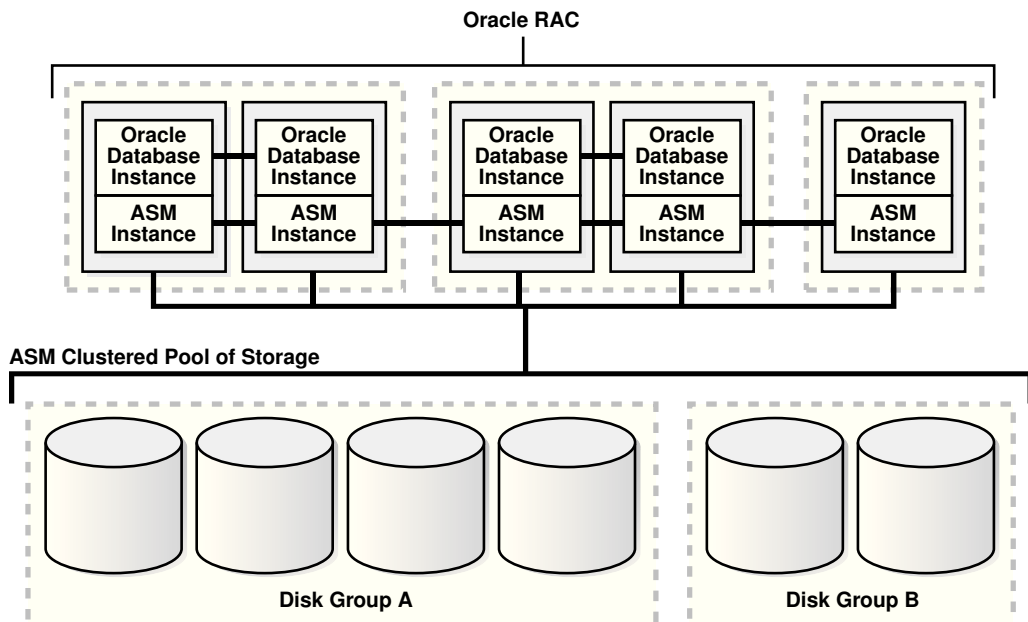
In [Figure 1](#), there are two disk groups: one disk group has four disks and the other has two disks. The database can access both disk groups. The configuration in [Figure 1](#) shows multiple database instances, but only one Oracle ASM instance is needed to serve the multiple database instances.

Figure 1 Oracle ASM for Single-Instance Oracle Databases



[Figure 2](#) shows an Oracle ASM cluster in an Oracle RAC environment where Oracle ASM provides a clustered pool of storage. There is one Oracle ASM instance for each node serving multiple Oracle RAC or single-instance databases in the cluster. All of the databases are consolidated and share the same two Oracle ASM disk groups.

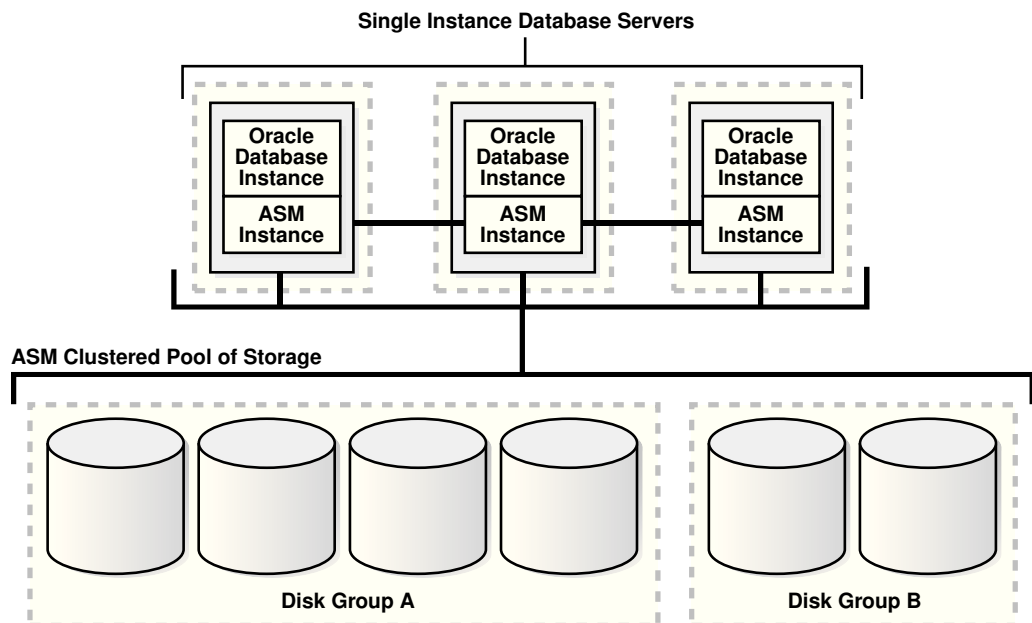
Figure 2 Oracle ASM Cluster Configuration with Oracle RAC



A clustered storage pool can be shared by multiple single-instance Oracle Databases as shown in [Figure 3](#). In this case, multiple databases share common disk groups. A shared Oracle ASM storage pool is achieved by using Oracle Clusterware. However, in such environments an Oracle RAC license is not required.

To share a disk group among multiple nodes, you must install Oracle Clusterware on all of the nodes, regardless of whether you install Oracle RAC on the nodes. Oracle ASM instances that are on separate nodes do not need to be part of an Oracle ASM cluster. However, if the Oracle ASM instances are not part of an Oracle ASM cluster, they cannot communicate with each other. Multiple nodes that are not part of an Oracle ASM cluster cannot share a disk group.

Figure 3 Oracle ASM Cluster with Single-Instance Oracle Databases



For information about Oracle Flex ASM configurations, refer to [“Managing Oracle Flex ASM”](#).

About Oracle ASM Disk Groups

A disk group consists of multiple disks and is the fundamental object that Oracle ASM manages. Each disk group contains the metadata that is required for the management of space in the disk group. Disk group components include disks, files, and allocation units.

Files are allocated from disk groups. Any Oracle ASM file is completely contained within a single disk group. However, a disk group might contain files belonging to several databases and a single database can use files from multiple disk groups. For most installations you need only a small number of disk groups, usually two, and rarely more than three. For more information about managing disk groups, see [Administering Oracle ASM Disk Groups](#).

About Mirroring and Failure Groups

Mirroring protects data integrity by storing copies of data on multiple disks. When you create a disk group, you specify an Oracle ASM disk group type based on one of the following three redundancy levels:

- **Normal** for 2-way mirroring
- **High** for 3-way mirroring
- **External** to not use Oracle ASM mirroring, such as when you configure hardware RAID for redundancy

The redundancy level controls how many disk failures are tolerated without dismounting the disk group or losing data. The disk group type determines the mirroring levels with which Oracle creates files in a disk group. For information about disk group types and templates, see [“Managing Disk Group Templates”](#).

Oracle ASM mirroring is more flexible than traditional RAID mirroring. For a disk group specified as `NORMAL` redundancy, you can specify the redundancy level for each file. For example, two files can share the same disk group with one file being mirrored while the other is not.

When Oracle ASM allocates an extent for a mirrored file, Oracle ASM allocates a primary copy and a mirror copy. Oracle ASM chooses the disk on which to store the mirror copy in a different failure group than the primary copy. Failure groups are used to place mirrored copies of data so that each copy is on a disk in a different failure group. The simultaneous failure of all disks in a failure group does not result in data loss.

You define the failure groups for a disk group when you create an Oracle ASM disk group. After a disk group is created, you cannot alter the redundancy level of the disk group. If you omit the failure group specification, then Oracle ASM automatically places each disk into its own failure group, except for disk groups containing disks on Oracle Exadata cells. Normal redundancy disk groups require at least two failure groups. High redundancy disk groups require at least three failure groups. Disk groups with external redundancy do not use failure groups.

For more information about mirroring and failure groups, see [“Mirroring_ Redundancy_ and Failure Group Options”](#).

About Oracle ASM Disks

Oracle ASM disks are the storage devices that are provisioned to Oracle ASM disk groups. Examples of Oracle ASM disks include:

- A disk or partition from a storage array
- An entire disk or the partitions of a disk
- Logical volumes
- Network-attached files (NFS)

When you add a disk to a disk group, you can assign an Oracle ASM disk name or Oracle ASM assigns the Oracle ASM disk name automatically. This name is different from the path name used by the operating system. In a cluster, a disk may be assigned different operating system device names on different nodes, but the disk has the same Oracle ASM disk name on all of the nodes. In a cluster, an Oracle ASM disk must be accessible from all of the instances that share the disk group.

Oracle ASM spreads the files proportionally across all of the disks in the disk group. This allocation pattern maintains every disk at the same capacity level and ensures that all of the disks in a disk group have the same I/O load. Because Oracle ASM load balances among all of the disks in a disk group, different Oracle ASM disks should not share the same physical drive.

About Oracle ASM Allocation Units

Every Oracle ASM disk is divided into allocation units (AU). An allocation unit is the fundamental unit of allocation within a disk group. A file extent consists of one or more allocation units. An Oracle ASM file consists of one or more file extents.

When you create a disk group, you can set the Oracle ASM allocation unit size with the `AU_SIZE` disk group attribute. The values can be 1, 2, 4, 8, 16, 32, or 64 MB, depending on the specific disk group compatibility level. Larger AU sizes typically provide performance advantages for data warehouse applications that use large sequential reads.

Refer to [Example 1](#) for an example that shows how the `AU_SIZE` is specified with the `CREATE DISKGROUP` SQL statement. For information about allocation unit sizes and disk group compatibility attributes, see “[Features Enabled By Disk Group Compatibility Attribute Settings](#)”.

See Also:

Articles at [My Oracle Support \(https://support.oracle.com\)](https://support.oracle.com) for additional information about allocation units and Oracle ASM

About Oracle ASM Files

Files that are stored in Oracle ASM disk groups are called Oracle ASM files. Each Oracle ASM file is contained within a single Oracle ASM disk group. Oracle Database communicates with Oracle ASM in terms of files. This is similar to the way Oracle Database uses files on any file system. You can store the various file types in Oracle ASM disk groups, including:

- Control files
- Data files, temporary data files, and data file copies
- SPFILEs
- Online redo logs, archive logs, and Flashback logs
- RMAN backups
- Disaster recovery configurations
- Change tracking bitmaps
- Data Pump dumpsets

Oracle ASM automatically generates Oracle ASM file names as part of file creation and tablespace creation. Oracle ASM file names begin with a plus sign (+) followed by a disk group name. You can specify user-friendly aliases for Oracle ASM files and create a hierarchical directory structure for the aliases.

The following sections describe the Oracle ASM file components:

- [Understanding Oracle ASM Extents](#)
- [Understanding Oracle ASM Striping](#)
- [About Oracle ASM File Templates](#)

Understanding Oracle ASM Extents

The contents of Oracle ASM files are stored in a disk group as a set, or collection, of **extents** that are stored on individual disks within disk groups. Each extent resides on an individual disk. Extents consist of one or more allocation units (AU). To accommodate increasingly larger files, Oracle ASM uses variable size extents.

Variable size extents enable support for larger Oracle ASM data files, reduce SGA memory requirements for very large databases, and improve performance for file create and open operations. The initial extent size equals the disk group allocation unit size and it increases by a factor of 4 or 16 at predefined thresholds. The various extent sizes are described in this section.

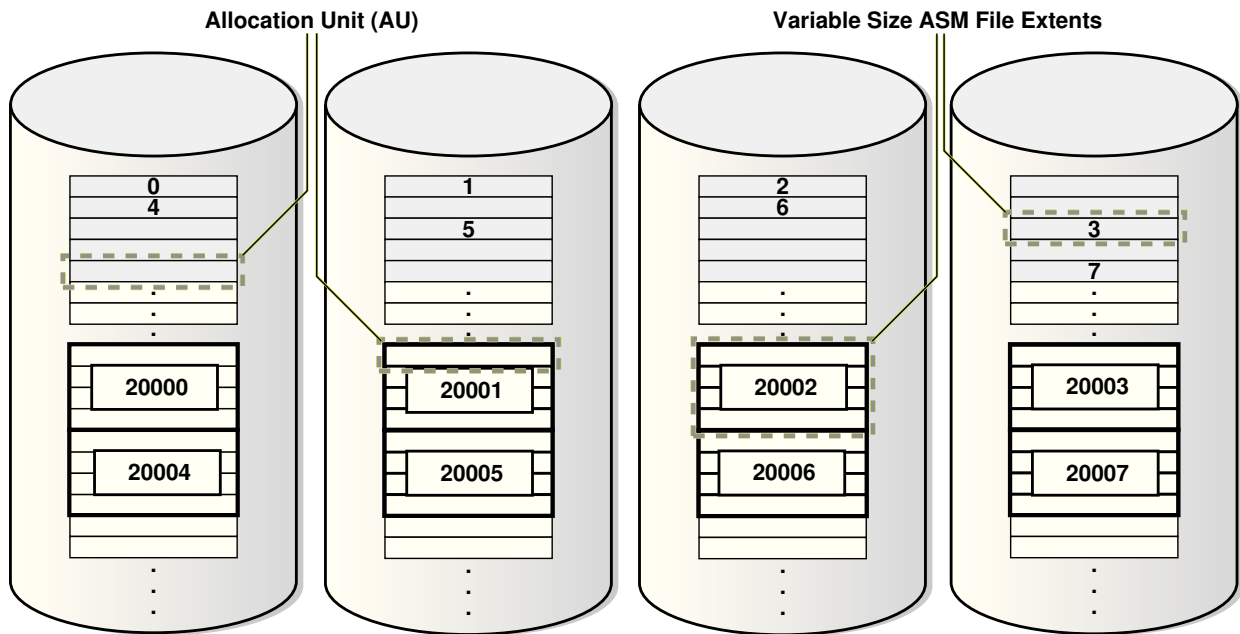
For disk groups with AU size less than 4 MB:

- Extent size always equals the disk group AU size for the first 20000 extent sets (0 - 19999).
- Extent size equals 4*AU size for the next 20000 extent sets (20000 - 39999).
- Extent size equals 16*AU size for the next 20000 and higher extent sets (40000+).

For disk groups with AU size greater than or equal to 4 MB and the disk group RDBMS compatibility greater than or equal to 11.2.0.4, the counts for extents of sizes (the disk group AU size, 4*AU size, or 16*AU size) are calculated using the application block size to support maximum file size.

The extent sizing feature is automatic for newly created and resized data files when specific disk group compatibility attributes are set to 11.1 or higher. For information about compatibility attributes, see “[Disk Group Compatibility](#)”.

[Figure 4](#) shows the Oracle ASM file extent relationship with allocation units. The first eight extents (0 to 7) are distributed on four Oracle ASM disks and are equal to the AU size. After the first 20000 extent sets, the extent size becomes 4*AU for the next 20000 extent sets (20000 - 39999). This is shown as bold rectangles labeled with the extent set numbers 20000 to 20007, and so on. The next increment for an Oracle ASM extent is 16*AU (not shown in [Figure 4](#)).

Figure 4 Oracle ASM File Allocation in a Disk Group

Understanding Oracle ASM Striping

Oracle ASM striping has two primary purposes:

- To balance loads across all of the disks in a disk group
- To reduce I/O latency

Coarse-grained striping provides load balancing for disk groups while fine-grained striping reduces latency for certain file types by spreading the load more widely.

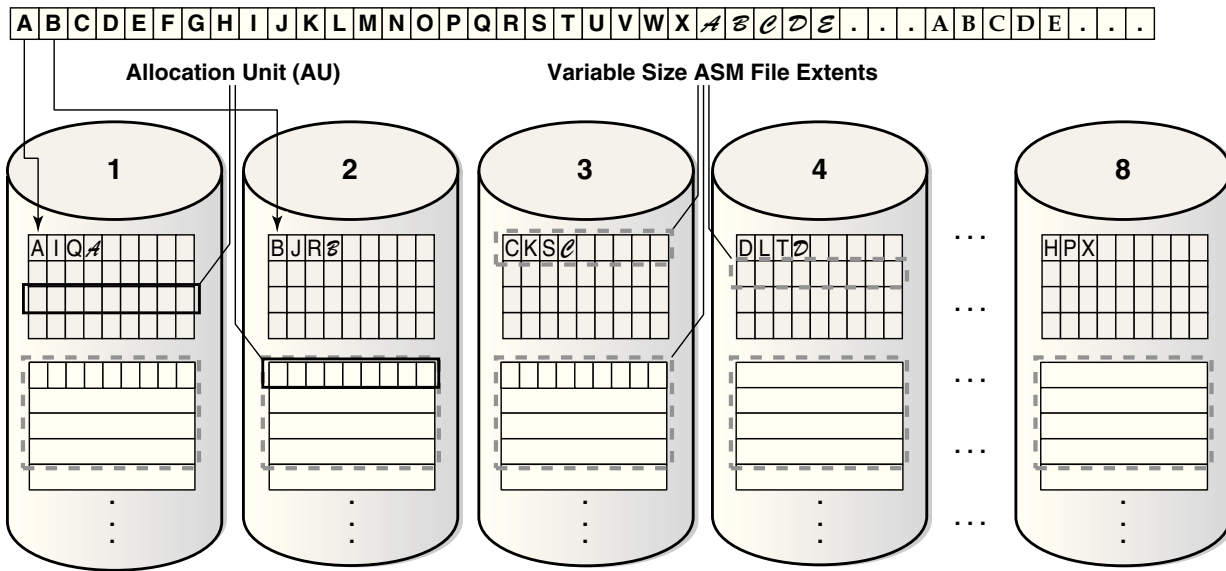
To stripe data, Oracle ASM separates files into stripes and spreads data evenly across all of the disks in a disk group. The fine-grained stripe size always equals 128 KB in any configuration; this provides lower I/O latency for small I/O operations. The coarse-grained stripe size is always equal to the AU size (not the data extent size).

[Figure 5](#) and [Figure 6](#) are illustrations of Oracle ASM file striping. In both illustrations, the allocation unit size has been set to 1 M (`AU_SIZE = 1M`) for the disk group which consists of 8 disks. The instance is Oracle ASM 11g Release 2 (11.2) and the disk group compatibility attributes for ASM and RDBMS have been set to 11.2, so variable extents are shown in the graphic after the first 20,000 extents. For the first 20,000 extents, the extent size is 1 M and equals one allocation unit (AU). For the next 20,000 extents, the extent size is 4 M and equals 4 AUs.

To identify the stripe chunks of the file, they have been labeled A..X (24 letters) using different fonts for successive series of A..X until all the chunks have been identified.

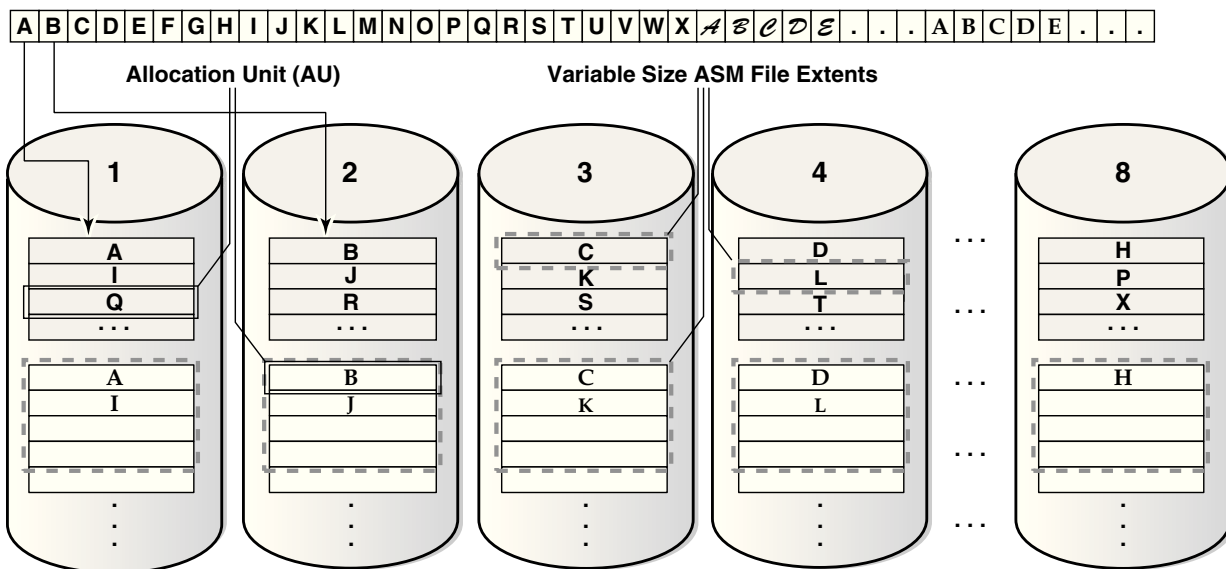
In [Figure 5](#), the file is striped in 128 K chunks (labeled A..X) with each 128 K chunk stored in an extent, starting at the first extent in disk 1, then the first extent in disk 2, and then continuing in a round-robin pattern through all the disks until the entire file has been striped. As shown in this example, the striping chunks first fill up the first extent of each disk, then the second extent of each disk, and so on until the entire file has been striped.

Figure 5 Oracle ASM Fine-Grained Striping



In [Figure 6](#), the file is striped in 1 M chunks (labeled A..X) with each 1 M chunk stored uniquely in an extent, starting at the first extent in disk 1, then the first extent in disk 2, and then continuing in a round-robin pattern through all the disks until the entire file has been striped. For the first 20,000 extents where the AU equals the extent size (1 M), the stripe equals the extent size and allocation unit size. For the variable extents, where an extent is composed of multiple allocation units, the file stripe is located in an AU of the extent. The striping chunks are placed in the allocation units of the first extents of all the disks before the striping continues to the next extent.

Figure 6 Oracle ASM Coarse-Grained Striping



About Oracle ASM File Templates

Templates are collections of attribute values that are used to specify disk regions, file mirroring, and [striping](#) attributes for an Oracle ASM file when it is created. When creating a file, you can include a template name and assign desired attributes based on an individual file rather than the file type.

A default template is provided for every Oracle file type, but you can customize templates to meet unique requirements. Each disk group has a default template associated with each file type.

For more information about Oracle ASM templates, see [“Managing Disk Group Templates”](#).

Understanding Oracle ASM Disk Group Administration

This section describes Oracle ASM disk group administration and it contains the following topics:

- [About Discovering Disks](#)
- [About Mounting and Dismounting Disk Groups](#)
- [About Adding and Dropping Disks](#)
- [About Online Storage Reconfigurations and Dynamic Rebalancing](#)

About Discovering Disks

The disk discovery process locates the operating system names for disks that Oracle ASM can access. Disk discovery finds all of the disks that comprise a disk group to be mounted. The set of discovered disks also includes disks that could be added to a disk group.

An Oracle ASM instance requires an `ASM_DISKSTRING` initialization parameter value to specify its discovery strings. Only path names that the Oracle ASM instance has permission to open are discovered. The exact syntax of a discovery string depends various factors, such as the platform and whether Oracle Exadata disks are used. The path names that an operating system accepts are always usable as discovery strings.

For information about the `ASM_DISKSTRING` initialization parameter, refer to [“ASM_DISKSTRING”](#). For information about disk discovery, refer to [“Oracle ASM Disk Discovery”](#). For information about Oracle ASM Filter Driver, refer to [“Oracle ASM Filter Driver”](#).

About Mounting and Dismounting Disk Groups

A disk group must be mounted by a local Oracle ASM instance before database instances can access the files in the disk group. Mounting the disk group requires discovering all of the disks and locating the files in the disk group that is being mounted.

You can explicitly dismount a disk group. Oracle reports an error if you attempt to dismount a disk group without the `force` option when any of the disk group files are open. It is possible to have disks fail in excess of the Oracle ASM redundancy setting. If this happens, then the disk group is forcibly dismounted. If the disk group is forcibly dismounted, a database cannot access files in the disk group.

For more information about disk groups, see [“Mounting and Dismounting Disk Groups”](#).

About Adding and Dropping Disks

You can add a disk to an existing disk group to add space and to improve throughput. The specified discovery string identifies the disk or disks that you could add. The disks that you add must be discovered by every Oracle ASM instance using its

ASM_DISKSTRING initialization parameter. After you add a disk, Oracle ASM rebalancing operations move data onto the new disk. To minimize the rebalancing I/O, it is more efficient to add multiple disks at the same time.

You can drop a disk from a disk group if it fails or to re-purpose capacity. Use the Oracle ASM disk name to drop a disk, not the discovery string device name. If an error occurs while writing to a disk, then Oracle ASM drops the disk automatically.

For more information about altering disk group membership, see “[Altering Disk Groups](#)”.

About Online Storage Reconfigurations and Dynamic Rebalancing

Rebalancing a disk group moves data between disks to ensure that every file is evenly spread across all of the disks in a disk group. When all of the files are evenly dispersed, all of the disks are evenly filled to the same percentage; this ensures load balancing. Rebalancing does not relocate data based on I/O statistics nor is rebalancing started based on I/O statistics. Oracle ASM rebalancing operations are controlled by the size of the disks in a disk group.

Oracle ASM automatically initiates a rebalance after storage configuration changes, such as when you add, drop, or resize disks. The power setting parameter determines the speed with which rebalancing operations occur.

You can manually start a rebalance to change the power setting of a running rebalance. A rebalance is automatically restarted if the instance on which the rebalancing is running stops. Databases can remain operational during rebalancing operations.

You can minimize the impact on database performance with the setting of the ASM_POWER_LIMIT initialization parameter. For more information about the power limit setting, see “[ASM_POWER_LIMIT](#)”. For more information about disk rebalancing, see “[Manually Rebalancing Disk Groups](#)”.

Exploring Considerations for Oracle ASM Storage

This chapter discusses issues to consider about the storage subsystem before you configure Oracle Automatic Storage Management (Oracle ASM). When preparing your storage to use Oracle ASM, first determine the storage option for your system and then prepare the disk storage for your specific operating system environment.

When configuring your system's storage, you must consider the initial capacity of the system and your plans for future growth. Oracle ASM simplifies the task of accommodating growth. However, your growth plans can affect choices, such as the size of the Oracle ASM disks. You must also consider that I/O performance depends on the interconnect between the storage and host, not just the storage disks. As you scale up the number of nodes in a cluster, you must also scale up the storage subsystem.

This chapter contains the following topics:

- [Storage Resources for Disk Groups](#)
- [Oracle ASM and Multipathing](#)
- [Recommendations for Storage Preparation](#)
- [Storage Device Path and Permission Persistence](#)

Storage Resources for Disk Groups

You can create an Oracle ASM disk group using one of the following storage resources:

- **Disk Partition**

A disk [partition](#) can be the entire disk drive or a section of a disk drive. However, the Oracle ASM disk cannot be in a partition that includes the partition table because the partition table would be overwritten.
- **Logical Unit Number (LUN)**

A LUN is a disk presented to a computer system by a storage array. Oracle recommends that you use hardware RAID functionality to create LUNs. Storage hardware RAID 0+1 or RAID5, and other RAID configurations, can be provided to Oracle ASM as Oracle ASM disks.
- **Logical Volume**

A logical [volume](#) is supported in less complicated configurations where a logical volume is mapped to a LUN, or a logical volume uses disks or raw partitions. Logical volume configurations are not recommended by Oracle because they create

a duplication of functionality. Oracle also does not recommended using logical [volume managers](#) for mirroring because Oracle ASM provides mirroring.

- **Network File System (NFS)**

An Oracle ASM disk group can be created from NFS files, including Oracle Direct NFS (dNFS), such as whole disks, partitions, and LUNs. The NFS files that are provisioned to a disk group may be from multiple NFS servers to provide better load balancing and flexible capacity planning.

You can use Direct NFS to store data files, but is not supported for Oracle Clusterware files. To install Oracle Real Application Clusters (Oracle RAC) on Windows using Direct NFS, you must also have access to a shared storage method other than NFS for Oracle Clusterware files.

See Also:

Oracle Grid Infrastructure Installation Guide for your operating system for information about Oracle Direct NFS

Note:

- Oracle ASM Dynamic Volume Manager (Oracle ADVM) volumes and Oracle Automatic Storage Management Cluster File System (Oracle ACFS) file systems are currently not supported on disk groups that have been created from NFS or Common Internet File System (CIFS) files. However, Oracle ACFS file systems may be exported as NFS or CIFS file systems to network clients in some cases. Samba/CIFS clients on Windows cannot use ACLs when interfacing with Oracle ACFS Linux, Solaris, or AIX servers.
 - Mounting loopback file systems over Oracle ACFS files is not supported.
 - Block or raw devices are not supported by Oracle Universal Installer (OUI) or Database Configuration Assistant (DBCA).
-
-

The procedures for preparing storage resources for Oracle ASM are:

- Identify or create the storage devices for Oracle ASM by identifying all of the storage resource device names that you can use to create an Oracle ASM disk group. For example, on Linux systems device names are typically presented from the `/dev` directory with the `/dev/device_name_identifier` name syntax.

- Change the ownership and the permissions on storage device resources.

For example, the following steps are required on Linux systems:

- Change the user and group ownership of devices, such as `grid:asmadmin`
For information about Oracle ASM privileges, see “[About Privileges for Oracle ASM](#)”.
- Change the device permissions to read/write

Note:

To ensure that ownership and permission settings are persistent, you can use `udev` to ensure that the disks do not revert to root ownership when the systems restart.

After you have configured Oracle ASM, ensure that disk discovery has been configured correctly by setting the `ASM_DISKSTRING` initialization parameter. For information about the `ASM_DISKSTRING` parameter, see “[ASM_DISKSTRING](#)”.

Note:

Setting the ownership to `oracle:dba` is one example that corresponds to the default settings. A nondefault installation may require different settings. In general, the owner of the disk devices should be the same as the owner of the Oracle binary software. The group ownership should be `OSDBA` of the Oracle ASM instance, which is defined at installation. For information about Oracle ASM privileges, see “[About Privileges for Oracle ASM](#)”.

For detailed information about preparing disks for an Oracle ASM installation, refer to your platform-specific installation guide for Oracle Database, Oracle Clusterware, and Oracle Real Application Clusters (Oracle RAC).

See Also:

Oracle Exadata documentation for information about preparing Oracle Exadata storage

Oracle ASM and Multipathing

Multipathing solutions provide failover by using redundant physical path components. These components include adapters, cables, and switches that reside between the server and the storage subsystem. If one or more of these components fails, then applications can still access their data, eliminating a single point of failure with the [Storage Area Network \(SAN\)](#), Host Bus Adapter, interface cable, or host port on a multiported storage array.

Multipathing is a software technology implemented at the operating system device driver level. Multipathing creates a pseudo device to facilitate the sharing and balancing of I/O operations across all of the available I/O paths. Multipathing also improves system performance by distributing the I/O load across all available paths, providing a higher level of data availability through automatic failover and failback.

Although Oracle ASM is not designed with multipathing functionality, Oracle ASM does operate with multipathing technologies. Multipathing technologies are available from many sources. Storage vendors offer multipathing products to support their specific storage products, while software vendors usually develop multipathing products to support several server platforms and storage products.

See Also:

Your storage or software vendor multipathing documentation for more information about multipathing options for specific platforms and storage products

With Oracle ASM, you can ensure the discovery of a multipath disk by setting the value of the `ASM_DISKSTRING` initialization parameter to a pattern that matches the pseudo devices that represents the multipath disk. When I/O is sent to the pseudo device, the multipath driver intercepts it and provides load balancing to the underlying subpaths.

If Oracle ASM discovers multiple paths to the same disk device, Oracle ASM then raises an error. Because a single disk can appear multiple times in a multipath configuration, you must configure Oracle ASM to discover only the multipath disk.

For information about disk discovery, see “[Oracle ASM Disk Discovery](#)”.

See Also:

- Articles at [My Oracle Support \(https://support.oracle.com\)](https://support.oracle.com) for information about Oracle ASM and Multipathing
 - Your platform-specific installation guide for information about configuring multipathing for your system
-
-

Recommendations for Storage Preparation

The following are guidelines for preparing storage for use with Oracle ASM:

- Configure two disk groups, one for data and the other for the fast recovery area.

See Also:

- *Oracle Database Backup and Recovery User's Guide* for information about configuring the fast recovery area
 - *Oracle Database Administrator's Guide* for information about specifying a fast recovery area
-
-

- The number of LUNs (Oracle ASM disks) for each disk group should be at least equal to four times the number of active I/O paths. For example, if a disk group has two active I/O paths, then minimum of eight LUNs should be used. The LUNs should be of equal size and performance for each disk group.

An I/O path is a distinct channel or connection between storage presenting LUNs and the server. An *active* I/O path is an I/O path in which the I/O load on a LUN is multiplexed through multipathing software.

- Ensure that all Oracle ASM disks in a disk group have similar storage performance and availability characteristics. In storage configurations with mixed speed drives,

such as flash memory and hard disk drives (HDD), I/O performance is constrained by the slowest speed drive.

- Oracle ASM data distribution policy is capacity-based. Ensure that Oracle ASM disks in a disk group have the same capacity to maintain balance.
- Configure a minimum of three failure groups for normal redundancy disk groups and five failure groups for high redundancy disk groups to maintain the necessary number of copies of the Partner Status Table (PST) to ensure robustness with respect to storage hardware failures. For more information, refer to “[Oracle ASM Failure Groups](#)”.
- Create external redundancy disk groups when using high-end storage arrays. High-end storage arrays generally provide hardware RAID protection. Use Oracle ASM mirroring redundancy when not using hardware RAID, or when you need host-based volume management functionality, such as mirroring across storage systems. You can use Oracle ASM mirroring in configurations when mirroring between geographically-separated sites (extended clusters).
- Minimize I/O contention between Oracle ASM disks and other applications by dedicating disks in Oracle ASM disk groups.
- Choose a hardware RAID stripe size that is a power of 2 and less than or equal to the size of the Oracle ASM allocation unit.
- Use the Oracle ASM Filter Driver feature to provide consistent device naming and permission persistency.

See Also:

- The Oracle Cloud Storage page on the Oracle Technology Network website at <http://www.oracle.com/technetwork/database/cloud-storage/index.html> for more information about Oracle ASM
 - Information about Oracle ASM Filter Driver at “[Oracle ASM Filter Driver](#)”
-
-

Storage Device Path and Permission Persistence

Before installation, or before configuring new storage devices to use with Oracle ASM, administrators must configure storage device names and ownership to ensure that storage paths and ownership persist after system restarts. Use Oracle ASM Filter Driver to maintain permissions and manage device paths. On Oracle Solaris, you can also use the Solaris I/O multipathing features to maintain permissions and device paths.

See Also:

Oracle Grid Infrastructure Installation Guide for your operating system for more information about configuring storage devices for path and permission persistence.

Part II

Oracle ASM Instances and Disk Groups

Part II discusses the administration of Oracle ASM instances and disk groups in the following chapters:

- [Administering Oracle ASM Instances](#)
- [Administering Oracle ASM Disk Groups](#)
- [Administering Oracle ASM Files_ Directories_ and Templates](#)
- [Using Views to Display Oracle ASM Information](#)
- [Administering Oracle ASM with Oracle Enterprise Manager](#)
- [Performing Oracle ASM Data Migration with RMAN](#)
- [Managing Oracle ASM With ASMCA](#)
- [Managing Oracle ASM with ASMCMD](#)

Administering Oracle ASM Instances

This chapter describes how to administer Automatic Storage Management (Oracle ASM) instances. It explains how to configure Oracle ASM instance parameters and how to set Oracle Database parameters for use with Oracle ASM. The chapter also describes Oracle ASM upgrading, patching, and authentication for Oracle ASM instance access. You can also use procedures in this chapter to migrate a database to use Oracle ASM.

Administering an Oracle ASM instance is similar to administering an Oracle Database instance, but the process requires fewer procedures. You can use Oracle ASM Command Line Utility (ASMCMD) command-line interface, Oracle ASM Configuration Assistant (ASMCA), and SQL*Plus to perform Oracle ASM instance administration tasks.

This chapter contains the following topics:

- [Operating with Different Releases of Oracle ASM and Database Instances Simultaneously](#)
- [Initialization Parameters for Oracle ASM Instances](#)
- [Administration of Oracle ASM Instances](#)
- [Upgrading and Patching Oracle ASM](#)
- [Oracle ASM Filter Driver](#)
- [Authentication for Accessing Oracle ASM Instances](#)
- [Migration of a Database to Use Oracle ASM](#)

For a description of an Oracle ASM instance, see “[About Oracle ASM Instances](#)”.

Operating with Different Releases of Oracle ASM and Database Instances Simultaneously

Oracle Automatic Storage Management (Oracle ASM) in Oracle Database 12c Release 1 (12.1) supports Oracle Database 12c Release 1 (12.1) or older software versions, including Oracle Database 10g Release 1 (10.1).

Note:

- An Oracle ASM instance must be at Oracle ASM 12c Release 1 (12.1) to support Oracle Database 12c Release 1 (12.1).
 - See *Oracle Exadata documentation* for information about the Oracle Database versions that Oracle ASM 12c Release 1 (12.1) supports when Oracle Exadata storage is present.
-

There are additional compatibility considerations when using disk groups with different releases of Oracle ASM and database instances. For information about disk group compatibility attributes settings, see “[Disk Group Compatibility](#)”.

When using different software versions, the database instance supports Oracle ASM functionality of the earliest release in use. For example, an Oracle Database 10g Release 1 (10.1) database instance operating with an Oracle ASM 11g Release 2 (11.2) instance supports only Oracle ASM 10g Release 1 (10.1) features.

The `V$ASM_CLIENT` view contains the `SOFTWARE_VERSION` and `COMPATIBLE_VERSION` columns with information about the software version number and instance compatibility level.

- The `SOFTWARE_VERSION` column of `V$ASM_CLIENT` contains the software version number of the database or Oracle ASM instance for the selected disk group connection.
- The `COMPATIBLE_VERSION` column contains the setting of the `COMPATIBLE` parameter of the database or Oracle ASM instance for the selected disk group connection.

You can query the `V$ASM_CLIENT` view on both Oracle ASM and database instances. For an example showing a query on the `V$ASM_CLIENT` view, see [Example 4](#). For more information about the `V$ASM_CLIENT` and `V$ASM_*` views, see “[Views Containing Oracle ASM Disk Group Information](#)”.

Initialization Parameters for Oracle ASM Instances

This section discusses initialization parameter files and parameter settings for Oracle ASM instances. To install and initially configure an Oracle ASM instance, use Oracle Universal Installer (OUI) and Oracle ASM Configuration Assistant (ASMCA). Refer to your platform-specific *Oracle Grid Infrastructure Installation Guide* for details about installing and configuring Oracle ASM.

After an Oracle ASM instance has been installed on a single-instance Oracle Database or in an Oracle Real Application Clusters (Oracle RAC) environment, the final Oracle ASM configuration can be performed. Only a few Oracle ASM-specific instance initialization parameters must be configured. The default values are usually sufficient.

See Also:

The Oracle Cloud Storage page on the Oracle Technology Network website at <http://www.oracle.com/technetwork/database/cloud-storage/index.html> for more information about Oracle ASM best practices

This section contains the following topics:

- [About Initialization Parameter Files for an Oracle ASM Instance](#)
- [About Backing Up_ Copying_ and Moving an Oracle ASM Initialization Parameter File](#)
- [About Oracle ASM Initialization Parameter Settings](#)
- [About Automatic Memory Management for Oracle ASM](#)
- [Recommended Settings for Oracle ASM Initialization Parameters](#)
- [About Setting Database Initialization Parameters for Use with Oracle ASM](#)

See Also:

- *Oracle Database Reference* for information about initialization parameters
 - *Oracle Database Administrator's Guide* for information about initialization parameter files
-
-

About Initialization Parameter Files for an Oracle ASM Instance

When installing Oracle ASM in an Oracle Restart (standalone) configuration, Oracle Universal Installer (OUI) creates a separate server parameter file (SPFILE) and password file for the Oracle ASM instance. The ASM SPFILE is stored in a disk group during installation.

When installing Oracle ASM in a clustered Oracle ASM environment, OUI creates a single, shared SPFILE for Oracle ASM in a disk group.

When upgrading an Oracle ASM instance, if the ASM SPFILE was originally in a shared file system, then the upgraded Oracle ASM instance retains the SPFILE in the same location. If the original Oracle ASM instance used a PFILE, then after an upgrade the instance continues to use a PFILE.

You can use an SPFILE or a text-based initialization parameter file (PFILE) as the Oracle ASM instance parameter file. If you use an SPFILE in a clustered Oracle ASM environment, then you must place the SPFILE in a disk group or on a cluster file system. Oracle recommends that the Oracle ASM SPFILE is placed in a disk group. You cannot use a new alias created on an existing Oracle ASM SPFILE to start the Oracle ASM instance.

If you do not use a shared Oracle Grid Infrastructure home, then the Oracle ASM instance can use a PFILE. The same rules for file name, default location, and search order that apply to database initialization parameter files also apply to Oracle ASM initialization parameter files.

When an Oracle ASM instance searches for an initialization parameter file, the search order is:

1. The location of the initialization parameter file specified in the Grid Plug and Play (GPnP) profile
2. If the location has not been set in the GPnP profile, then the search order changes to:

- a. SPFILE in the Oracle ASM instance home

For example, the SPFILE for Oracle ASM has the following default path in the Oracle Grid Infrastructure home in a Linux environment:

```
$ORACLE_HOME/dbs/spfile+ASM.ora
```

- b. PFILE in the Oracle ASM instance home

Note:

A PFILE or SPFILE is required if your configuration uses nondefault initialization parameters for the Oracle ASM instance.

You can administer Oracle ASM initialization parameter files with SQL*Plus, ASMCA, and ASMCMD commands. For information about the ASMCA GUI and command-line interfaces, see [Managing Oracle ASM With ASMCA](#). For information about ASMCMD commands for managing an Oracle ASM SPFILE; such as `spbackup`, `spcopy`, and `spmmove`; see [“ASMCMD Instance Management Commands”](#).

See Also:

- *Oracle Database Administrator's Guide* for more information about creating and maintaining initialization parameter files
 - *Oracle Database SQL Language Reference* for information about creating an SPFILE with the `CREATE SPFILE` SQL statement
-
-

About Backing Up, Copying, and Moving an Oracle ASM Initialization Parameter File

You can back up, copy, or move an Oracle ASM SPFILE with the ASMCMD `spbackup`, `spcopy`, or `spmmove` commands. In addition, you can use the SQL `CREATE SPFILE` to create an Oracle ASM SPFILE when connected to the Oracle ASM instance.

You can also copy and move an Oracle ASM PFILE with the commands available on the specific platform, such as `cp` for Linux.

After copying or moving an SPFILE or PFILE, you must restart the instance with the SPFILE or PFILE in the new location to use that SPFILE or PFILE.

This section contains the following topics:

- [Creating, Copying, and Moving an SPFILE Into a Disk Group](#)
- [Making a Back Up Copy of an Oracle ASM SPFILE in a Disk Group](#)

For information about ASMCMD commands for managing an SPFILE, see [“spbackup”](#), [“spcopy”](#), and [“spmmove”](#).

See Also:

- *Oracle Database Administrator's Guide* for more information about creating and maintaining initialization parameter files
 - *Oracle Database SQL Language Reference* for information about creating an SPFILE with the `CREATE SPFILE` SQL statement
 - *Oracle Real Application Clusters Installation Guide* for information about Grid Plug and Play (GPnP)
-

Creating, Copying, and Moving an SPFILE Into a Disk Group

If the `COMPATIBLE .ASM` disk group attribute is set to 11.2 or greater for a disk group, you can create, copy, or move an Oracle ASM SPFILE into the disk group.

For example, after upgrading an instance from Oracle ASM 11g Release 1 (11.1) to Oracle ASM 11g Release 2 (11.2), you could place the Oracle ASM SPFILE in a disk group that has `COMPATIBLE .ASM` set to 11.2. For information about disk group compatibility attributes, see [“Disk Group Compatibility”](#).

In the following steps, assume an Oracle ASM 11g Release 2 (11.2) instance is using a PFILE stored in `$ORACLE_HOME/dbs/asmprofile.ora`. You can use the SQL `CREATE SPFILE` statement to create an SPFILE from a PFILE stored in a local or shared file system. If a PFILE does not exist, then it could be created with the SQL `CREATE PFILE` statement.

To create an SPFILE in a disk group, perform the following steps:

1. Connect to the Oracle ASM instance.

For example:

```
$ sqlplus / as sysasm
```

2. Create an SPFILE in a disk group that has `COMPATIBLE .ASM` set to 11.2 with the SQL `CREATE SPFILE` statement.

For example, create an Oracle ASM SPFILE from the existing PFILE.

```
SQL> CREATE SPFILE = '+DATA/asmprofile.ora'
      FROM PFILE = '$ORACLE_HOME/dbs/asmprofile.ora';
```

The `CREATE SPFILE` statement also updates the Grid Plug and Play (GPnP) profile. You can check the location of the Oracle ASM SPFILE in the GPnP profile with the ASMCMD `spget` command. See [“spget”](#).

3. Restart the Oracle ASM instance so that the instance reads the SPFILE in the new location.

For information on shutting down and starting up an Oracle ASM instance, see [“About Starting Up an Oracle ASM Instance”](#) and [“About Shutting Down an Oracle ASM Instance”](#).

Making a Back Up Copy of an Oracle ASM SPFILE in a Disk Group

This section describes the steps to make a back up copy of an Oracle ASM SPFILE in another disk group using the ASMCMD commands. If necessary, then the backup copy can be used to restore the Oracle ASM SPFILE.

The source and target disk groups must have the disk group attribute `COMPATIBLE.ASM` set to 11.2 or higher.

To make a copy of the Oracle ASM SPFILE in another disk group with the `spcopy` command perform the following steps:

1. Locate the Oracle ASM SPFILE using the `ASMCMD spget` command.

For example:

```
ASMCMD [+] > spget
+DATA/ASM/ASMPARAMETERFILE/registry.253.849343867
```

2. Copy the Oracle ASM SPFILE to another disk group with `spcopy` command.

For example:

```
ASMCMD [+] > spcopy +DATA/ASM/ASMPARAMETERFILE/registry.253.849343867 +FRA/spfileCopyASM.ora
```

Running `spcopy` without the `-u` option does not update the location of the Oracle ASM SPFILE. You can use `spset` to set the location of the Oracle ASM SPFILE in the Grid Plug and Play (GPnP) profile.

3. List all the copies of the Oracle ASM SPFILE file contained in the FRA disk group using the `ASMCMD ls` command.

For example:

```
ASMCMD [+] > ls -l --absolutepath FRA/ASM/ASMPARAMETERFILE
Type          Redund  Striped  Time                Sys  Name
ASMPARAMETERFILE MIRROR COARSE   JUN 06 13:00:00    Y    +FRA/spfileCopyASM.ora => REGISTRY.
253.849533009
```

4. Verify the current location of the Oracle ASM SPFILE file with the `spget` command.

For example:

```
ASMCMD [+] > spget
+DATA/ASM/ASMPARAMETERFILE/registry.253.849343867
```

In the event that the current Oracle ASM SPFILE file in a disk group has been corrupted or that disk group is not accessible, you can use `spset` or `spcopy` with the `-u` option to restore the Oracle ASM SPFILE file using the backup copy that you have previously created.

For example:

```
ASMCMD [+] > spcopy -u +FRA/spfileCopyASM.ora +DATA2/ASM/spfileASM.ora
```

About Oracle ASM Initialization Parameter Settings

There are several initialization parameters that you must set for an Oracle ASM instance. You can set these parameters with Oracle ASM Configuration Assistant (ASMCA). You can also set some parameters after database creation using `SQL ALTER SYSTEM` or `ALTER SESSION` statements.

The Oracle ASM parameters use suitable defaults for most environments. You cannot use parameters with names that are prefixed with `ASM_*` in database instance parameter files.

About Automatic Memory Management for Oracle ASM

Automatic memory management automatically manages the memory-related parameters for both Oracle ASM and database instances with the `MEMORY_TARGET` parameter. Automatic memory management is enabled by default on an Oracle ASM instance, even when the `MEMORY_TARGET` parameter is not explicitly set. The default value used for `MEMORY_TARGET` is acceptable for most environments. This is the only parameter that you must set for complete Oracle ASM memory management. Oracle strongly recommends that you use automatic memory management for Oracle ASM.

If you do not set a value for `MEMORY_TARGET`, but you do set values for other memory related parameters, Oracle internally calculates the optimum value for `MEMORY_TARGET` based on those memory parameter values. You can also increase `MEMORY_TARGET` dynamically, up to the value of the `MEMORY_MAX_TARGET` parameter, just as you can do for the database instance.

Although it is not recommended, you can disable automatic memory management by either setting the value for `MEMORY_TARGET` to 0 in the Oracle ASM parameter file or by running an `ALTER SYSTEM SET MEMORY_TARGET=0` statement. When you disable automatic memory management, Oracle reverts to automatic shared memory management and automatic PGA memory management. To revert to Oracle Database 10g Release 2 (10.2) functionality to manually manage Oracle ASM SGA memory, also run the `ALTER SYSTEM SET SGA_TARGET=0` statement. Unless specified, the behaviors of the automatic memory management parameters in Oracle ASM instances behave the same as in Oracle Database instances.

Note:

- For a Linux environment, automatic memory management cannot work if `/dev/shm` is not available or is undersized. For more information, see *Oracle Database Administrator's Reference for Linux and UNIX-Based Operating Systems*. For information about platforms that support automatic memory management, see *Oracle Database Administrator's Guide*.
- The minimum `MEMORY_TARGET` for Oracle ASM is 1 GB. If you set `MEMORY_TARGET` lower, then Oracle increases the value for `MEMORY_TARGET` to 1 GB automatically.
- For the recommended settings of memory initialization parameters in an Oracle Exadata environment, refer to the Oracle Exadata documentation.

See Also:

- *Oracle Database Administrator's Guide* for more information about the functionality of automatic memory management for database instances, which varies from Oracle ASM
 - *Oracle Database Concepts* for an overview of memory management methods
-
-

Recommended Settings for Oracle ASM Initialization Parameters

This section contains information about the following initialization parameters for Oracle ASM:

- [ASM_DISKGROUPS](#)
- [ASM_DISKSTRING](#)
- [ASM_POWER_LIMIT](#)
- [ASM_PREFERRED_READ_FAILURE_GROUPS](#)
- [DB_CACHE_SIZE](#)
- [DIAGNOSTIC_DEST](#)
- [INSTANCE_TYPE](#)
- [LARGE_POOL_SIZE](#)
- [PROCESSES](#)
- [REMOTE_LOGIN_PASSWORDFILE](#)
- [SHARED_POOL_SIZE](#)

See Also:

Oracle Database Administrator's Guide for more information about creating and maintaining an initialization parameter file

ASM_DISKGROUPS

The `ASM_DISKGROUPS` initialization parameter specifies a list of disk group names that an Oracle ASM instance mounts at startup when the SQL `ALTER DISKGROUP ALL MOUNT` statement is issued. The Oracle ASM instance startup process executes `ALTER DISKGROUP ALL MOUNT` unless the `NOMOUNT` startup option is specified.

The default value of the `ASM_DISKGROUPS` parameter is a `NULL` string. For information about disk groups that are mounted at startup time, see [“About Mounting Disk Groups at Startup”](#).

The `ASM_DISKGROUPS` parameter is dynamic. If you are using a server parameter file (SPFILE), then you do not have to manually alter the value of `ASM_DISKGROUPS`. Oracle ASM automatically adds a disk group to the parameter when the disk group is successfully created or mounted. Oracle ASM also automatically removes a disk group from the parameter when the disk group is dropped or dismounted.

The following is an example of setting the `ASM_DISKGROUPS` parameter dynamically:

```
SQL> ALTER SYSTEM SET ASM_DISKGROUPS = DATA, FRA;
```

When using a text initialization parameter file (PFILE), you may edit the initialization parameter file to add the name of any disk group so that it is mounted automatically at instance startup. You must remove the name of any disk group that you no longer want automatically mounted.

The following is an example of the `ASM_DISKGROUPS` parameter in the initialization file:

```
ASM_DISKGROUPS = DATA, FRA
```

Note:

Issuing the `ALTER DISKGROUP...ALL MOUNT` or `ALTER DISKGROUP...ALL DISMOUNT` commands does not affect the value of `ASM_DISKGROUPS`.

For additional information about mounting Oracle ASM disk groups, see “[Mounting and Dismounting Disk Groups](#)”.

For Oracle Database 12c Release 1 or later, Oracle ASM configurations support up to 511 disk groups. Oracle ASM configurations with Oracle Database releases before 12c Release 1 can only support up to 63 disk groups.

See Also:

Oracle Database Reference for more information about the `ASM_DISKGROUPS` initialization parameter

ASM_DISKSTRING

The `ASM_DISKSTRING` initialization parameter specifies a comma-delimited list of strings that limits the set of disks that an Oracle ASM instance discovers. The discovery strings can include wildcard characters. Only disks that match one of the strings are discovered. The same disk cannot be discovered twice.

The discovery string format depends on the Oracle ASM library and the operating system that are in use. Pattern matching is supported. Refer to your operating system-specific installation guide for information about the default pattern matching.

For example on a Linux server, to limit the discovery process to only include disks that are in the `/dev/rdisk/mydisks` directory for an Oracle ASM instance that does not use Oracle ASM Filter Driver (Oracle ASMFd) or ASMLIB, set the `ASM_DISKSTRING` initialization parameter to:

```
/dev/rdisk/mydisks/*
```

The asterisk is required.

To limit the discovery process to only include disks that have a name that ends in `disk3` or `disk4`, you could set `ASM_DISKSTRING` as follows on a Linux system:

```
ASM_DISKSTRING = '/dev/rdisk/*disk3', '/dev/rdisk/*disk4'
```

The `?` character, when used as the first character of a path, expands to the Oracle home directory. Depending on the operating system, when you use the `?` character elsewhere in the path, it is a wildcard for one character.

The default value of the `ASM_DISKSTRING` parameter is a NULL string. A NULL value causes Oracle ASM to search a default path for all disks in the system to which the Oracle ASM instance has read and write access. The default search path is platform-specific. Refer to your operating system-specific installation guide for more information about the default search path.

Oracle ASM cannot use a disk unless all of the Oracle ASM instances in the cluster can discover the disk through one of their own discovery strings. The names do not have to be the same on every node, but all disks must be discoverable by all of the nodes in the cluster. This may require dynamically changing the initialization parameter to enable adding new storage.

For additional information about discovering disks, see [“Oracle ASM Disk Discovery”](#).

See Also:

- *Oracle Exadata documentation* for information about the Oracle ASM discovery string format for Oracle Exadata
 - *Oracle Database Reference* for more information about the `ASM_DISKSTRING` initialization parameter
-
-

ASM_POWER_LIMIT

The `ASM_POWER_LIMIT` initialization parameter specifies the default power for disk rebalancing in a disk group. The range of values is 0 to 1024. The default value is 1. A value of 0 disables rebalancing. Higher numeric values enable the rebalancing operation to complete more quickly, but might result in higher I/O overhead and more rebalancing processes.

- For disk groups that have the disk group ASM compatibility set to 11.2.0.2 or higher (for example, `COMPATIBLE.ASM = 11.2.0.2`), the operational range of values is 0 to 1024 for the rebalance power.
- For disk groups that have the disk group ASM compatibility set to less than 11.2.0.2, the operational range of values is 0 to 11 inclusive. If the value for `ASM_POWER_LIMIT` is larger than 11, a value of 11 is used for these disk groups.

You can also specify the power of the rebalancing operation in a disk group with the `POWER` clause of the `SQL ALTER DISKGROUP .. REBALANCE` statement. The range of allowable values for the `POWER` clause is the same for the `ASM_POWER_LIMIT` initialization parameter. If the value of the `POWER` clause is specified larger than 11 for a disk group with ASM compatibility set to less than 11.2.0.2, then a warning is displayed and a `POWER` value equal to 11 is used for rebalancing.

The specification of the power of the rebalancing operation in a disk group only affects rebalance operations, not new allocations to a disk group.

For information about the `ASM_POWER_LIMIT` initialization parameter, and the `POWER` clause, refer to [“Manually Rebalancing Disk Groups”](#) and [“Tuning Rebalance Operations”](#). For information about disk group compatibility, see [“Disk Group Compatibility”](#).

See Also:

- *Oracle Database Reference* for more information about the `ASM_POWER_LIMIT` initialization parameter
 - *Oracle Database SQL Language Reference* for more information about the `POWER` clause of the `SQL ALTER DISKGROUP REBALANCE` statement
-
-

ASM_PREFERRED_READ_FAILURE_GROUPS

The `ASM_PREFERRED_READ_FAILURE_GROUPS` initialization parameter value is a comma-delimited list of strings that specifies the failure groups that should be preferentially read by the given instance. The `ASM_PREFERRED_READ_FAILURE_GROUPS` parameter setting is instance specific. The default value is `NULL`. This parameter is generally used for clustered Oracle ASM instances and its value can be different on different nodes.

For example:

```
diskgroup_name1.failure_group_name1, ...
```

For more information about `ASM_PREFERRED_READ_FAILURE_GROUPS`, refer to [“Preferred Read Failure Groups”](#).

See Also:

- *Oracle Real Application Clusters Administration and Deployment Guide* for more information about configuring preferred disks in extended clusters
 - *Oracle Database Reference* for more information about the `ASM_PREFERRED_READ_FAILURE_GROUPS` initialization parameter
-
-

DB_CACHE_SIZE

You do not have to set a value for the `DB_CACHE_SIZE` initialization parameter if you use automatic memory management. The setting for the `DB_CACHE_SIZE` parameter determines the size of the buffer cache. This buffer cache stores metadata blocks. The default value for this parameter is suitable for most environments.

See Also:

- *Oracle Database Administrator's Guide* for more information about setting the `DB_CACHE_SIZE` initialization parameter
 - *Oracle Database Performance Tuning Guide* for more information about memory configuration
 - *Oracle Database Reference* for more information about the `DB_CACHE_SIZE` parameter
-
-

DIAGNOSTIC_DEST

The `DIAGNOSTIC_DEST` initialization parameter specifies the directory where diagnostics for an instance are located. The default value for an Oracle ASM instance is the `$ORACLE_BASE` directory for the Oracle Grid Infrastructure installation.

[Example 1](#) shows an example of the diagnostic directory for an Oracle ASM instance.

See Also:

- *Oracle Database Administrator's Guide* for more information about the `DIAGNOSTIC_DEST` initialization parameter and the fault diagnosability infrastructure.
 - *Oracle Database Reference* for more information about the `DIAGNOSTIC_DEST` parameter
-
-

Example 1 Sample diagnostic directory for an Oracle ASM instance

```
$ ls $ORACLE_BASE/diag/asm/+asm/+ASM
alert cdump hm incident incpkg ir lck metadata stage sweep trace
```

INSTANCE_TYPE

The following is an example of the `INSTANCE_TYPE` parameter in the initialization file:

```
INSTANCE_TYPE = ASM
```

In addition to values `asm` and `rdbms`, `INSTANCE_TYPE` can be set to `asmproxy` in an Oracle Flex ASM configuration. For more information about Oracle Flex ASM, refer to [“Managing Oracle Flex ASM”](#).

See Also:

Oracle Database Reference for more information about the `INSTANCE_TYPE` parameter

LARGE_POOL_SIZE

You do not have to set a value for the `LARGE_POOL_SIZE` initialization parameter if you use automatic memory management.

The setting for the `LARGE_POOL_SIZE` parameter is used for large allocations. The default value for this parameter is suitable for most environments.

See Also:

- *Oracle Database Administrator's Guide* for more information about setting the `LARGE_POOL_SIZE` initialization parameter
 - *Oracle Database Performance Tuning Guide* for more information about memory configuration
 - *Oracle Database Reference* for more information about the `LARGE_POOL_SIZE` parameter
-
-

PROCESSES

The `PROCESSES` initialization parameter affects Oracle ASM, but the default value is usually suitable. However, if multiple database instances are connected to an Oracle ASM instance, then you can use the following formulas, where n is the number of database instances connecting to the Oracle ASM instance.

In a non-Exadata environment, the recommended settings are:

- For $n < 10$, `PROCESSES` = $50 * n + 50$
- For $n \geq 10$, `PROCESSES` = $10 * n + 450$

In an Oracle Exadata environment, the recommended setting is `PROCESSES` = `MAX(450 + 10 * n, 1024)`.

See Also:

- *Oracle Database Administrator's Guide* for more information about setting the `PROCESSES` initialization parameter
 - *Oracle Database Reference* for more information about the `PROCESSES` parameter
-
-

REMOTE_LOGIN_PASSWORDFILE

The `REMOTE_LOGIN_PASSWORDFILE` initialization parameter specifies whether the Oracle ASM instance checks for a password file. This parameter operates the same for Oracle ASM and database instances.

See Also:

- *Oracle Database Administrator's Guide* for more information about setting the `REMOTE_LOGIN_PASSWORDFILE` initialization parameter
 - *Oracle Database Reference* for more information about the `REMOTE_LOGIN_PASSWORDFILE` parameter
-
-

SHARED_POOL_SIZE

You do not have to set a value for the SHARED_POOL_SIZE initialization parameter if you use automatic memory management. The setting for the SHARED_POOL_SIZE parameter determines the amount of memory required to manage the instance. The setting for this parameter is also used to determine the amount of space that is allocated for extent storage. The default value for this parameter is suitable for most environments.

See Also:

- *Oracle Database Administrator's Guide* for more information about setting the SHARED_POOL_SIZE initialization parameter
 - *Oracle Database Performance Tuning Guide* for more information about memory configuration
 - *Oracle Database Reference* for more information about the SHARED_POOL_SIZE parameter
-
-

About Setting Database Initialization Parameters for Use with Oracle ASM

When you do not use automatic memory management in a database instance, the SGA parameter settings for a database instance may require minor modifications to support Oracle ASM. When you use automatic memory management, the sizing data discussed in this section can be treated as informational only or as supplemental information to help determine the appropriate values that you should use for the SGA. Oracle highly recommends using automatic memory management.

See Also:

- *Oracle Database Administrator's Guide* for information about managing memory allocation in an Oracle Database instance
 - *Oracle Database Performance Tuning Guide* for more information about memory configuration and use
-
-

The following are configuration guidelines for SGA sizing on the database instance:

- PROCESSES initialization parameter—Add 16 to the current value
- LARGE_POOL_SIZE initialization parameter—Add an additional 600K to the current value
- SHARED_POOL_SIZE initialization parameter—Aggregate the values from the following queries to obtain the current database storage size that is either on Oracle ASM or stored in Oracle ASM. Next, determine the redundancy type and calculate the SHARED_POOL_SIZE using the aggregated value as input.

```
SELECT SUM(bytes)/(1024*1024*1024) FROM V$DATAFILE;  
SELECT SUM(bytes)/(1024*1024*1024) FROM V$LOGFILE a, V$LOG b  
WHERE a.group#=b.group#;
```

```
SELECT SUM(bytes)/(1024*1024*1024) FROM V$tempfile
WHERE status='ONLINE';
```

- For disk groups using external redundancy, every 100 GB of space needs 1 MB of extra shared pool plus 2 MB
- For disk groups using normal redundancy, every 50 GB of space needs 1 MB of extra shared pool plus 4 MB
- For disk groups using high redundancy, every 33 GB of space needs 1 MB of extra shared pool plus 6 MB

See Also:

- *Oracle Database Administrator's Guide* for information about managing memory allocation in an Oracle Database instance
 - *Oracle Database Performance Tuning Guide* for more information about memory configuration and use
-

Administration of Oracle ASM Instances

Oracle ASM is typically installed in an Oracle Grid Infrastructure home separate from the Oracle Database home. Only one Oracle ASM instance is supported on a server in a standard configuration; however, Oracle Flex ASM provides additional configuration options.

When managing an Oracle ASM instance, the administration activity should be performed in the Oracle Grid Infrastructure home.

This section describes how to administer Oracle ASM instances under the following topics:

- [Managing Oracle Flex ASM](#)
- [Using Oracle Restart](#)
- [About Starting Up an Oracle ASM Instance](#)
- [About Shutting Down an Oracle ASM Instance](#)
- [About Administering Oracle ASM Instances with Server Control Utility](#)
- [About Out of Place Upgrades](#)
- [About Configuring Oracle Grid Infrastructure with the Configuration Wizard](#)
- [About Active Session History Sampling for Oracle ASM](#)
- [About Oracle Home User on Windows](#)

Managing Oracle Flex ASM

Oracle Flex ASM enables Oracle ASM instances to run on a separate physical server from the database servers. This section discusses Oracle Flex ASM in the following topics:

- [Overview of Oracle Flex ASM](#)

- [About Setting Up Oracle Flex ASM](#)
- [Administering Oracle Flex ASM](#)

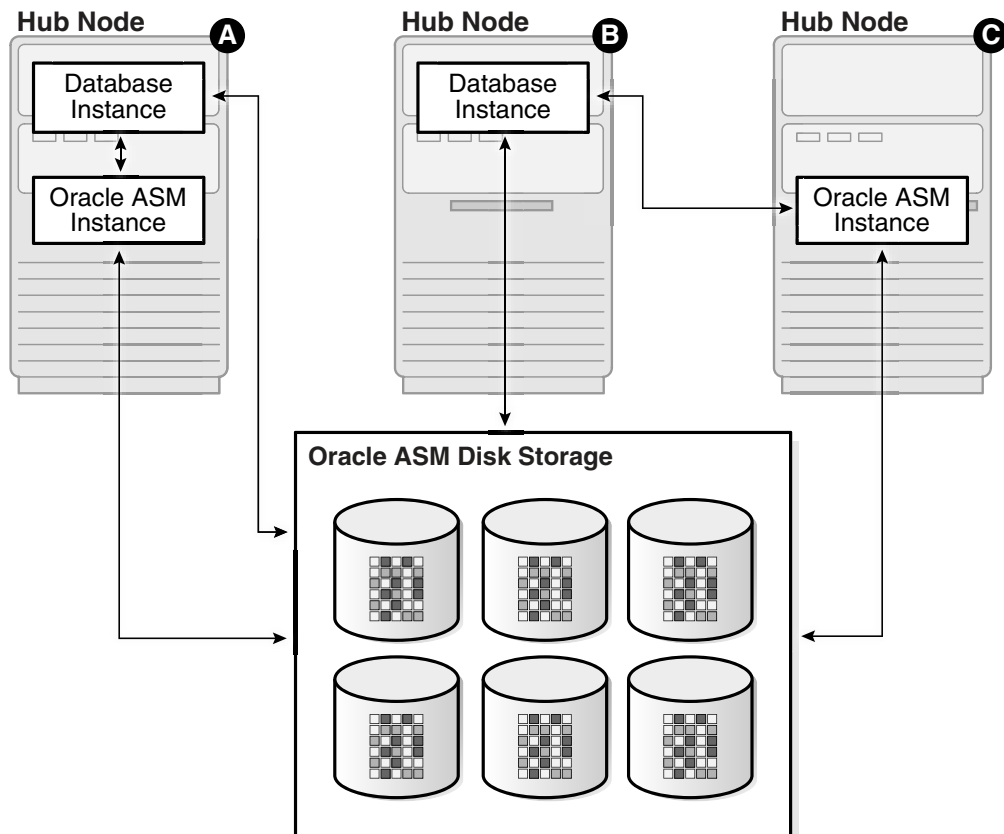
See Also:

Oracle Clusterware Administration and Deployment Guide for information about Oracle Flex Cluster support

Overview of Oracle Flex ASM

An Oracle ASM instance can operate in several configurations in Oracle Flex ASM, as shown in [Figure 1](#). This illustration shows the distinct modes of operation which are available for Oracle Flex ASM in Oracle ASM 12c Release 1 (12.1).

Figure 1 Oracle Flex ASM Configurations



Oracle Flex ASM enables an Oracle ASM instance to run on a separate physical server from the database servers. With this deployment, larger clusters of Oracle ASM instances can support more database clients while reducing the Oracle ASM footprint for the overall system.

When using Oracle Flex ASM, Oracle ASM clients are configured with direct access to storage.

With Oracle Flex ASM, you can consolidate all the storage requirements into a single set of disk groups. All these disk groups are mounted by and managed by a small set of Oracle ASM instances running in a single cluster. You can specify the number of Oracle ASM instances with a cardinality setting. The default is three instances.

A cluster is a set of nodes that provide group membership services. Each cluster has a name that is globally unique. Every cluster has one or more Hub nodes. The Hub nodes have access to Oracle ASM disks. Every cluster has at least one private network and one public network. If the cluster is going to use Oracle ASM for storage, it has at least one Oracle ASM network. A single network can be used as both a private and an Oracle ASM network. For security reasons, an Oracle ASM network should never be public. There can be only one Oracle Flex ASM configuration running within a cluster.

The configurations of Oracle ASM in Oracle Flex ASM are:

- Local Oracle ASM clients with direct access to Oracle ASM disks

With this mode (Standard Oracle ASM cluster), Oracle ASM continues to support existing standard architecture in which database clients are running with an Oracle ASM instance on the same host computer. The local client architecture is only supported on a Hub node. This mode is labeled **A** in [Figure 1](#).

In this configuration, the database instances are on the same Hub node as the Oracle ASM instance and are referred to as local Oracle ASM client instances. Oracle ASM metadata moves between Oracle ASM and the database instances. This client has direct I/O access to Oracle ASM disks.

Local mode does not use Oracle Flex ASM, so clusters configured with local Oracle ASM do not require an Oracle ASM network, nor do they contain other Oracle Flex ASM services.

- Oracle Flex ASM clients with direct access to Oracle ASM disks

With this mode, database clients that are running on Hub nodes of the Oracle ASM cluster access Oracle ASM remotely for metadata, but perform block I/O operations directly to Oracle ASM disks. The hosts running the Oracle ASM server and the remote database client must both be Hub nodes. A Hub node is a node in an Oracle ASM cluster that is tightly connected with other servers and has direct access to a shared disk. This mode is labeled **B** in [Figure 1](#).

In this configuration, the database instances are on different host computers than the nearby Oracle ASM instance and are referred to as Oracle ASM client instances. This Oracle ASM instance is shown on the node labeled **C** in [Figure 1](#). The databases are in the same Oracle ASM cluster as the Oracle ASM instance and the database instances are located on a Hub node. Oracle ASM metadata moves between Oracle ASM and the database instance. This client has direct I/O access to Oracle ASM disks.

Depending on the distribution of database instances and Oracle ASM instances, a database client may access Oracle ASM locally on the same node or remotely over the Oracle ASM network. This mode of operation is used by database clients on Hub nodes in the Oracle ASM cluster. Direct access mode is also the only Oracle Flex ASM configuration supported by Oracle ASM cluster file system.

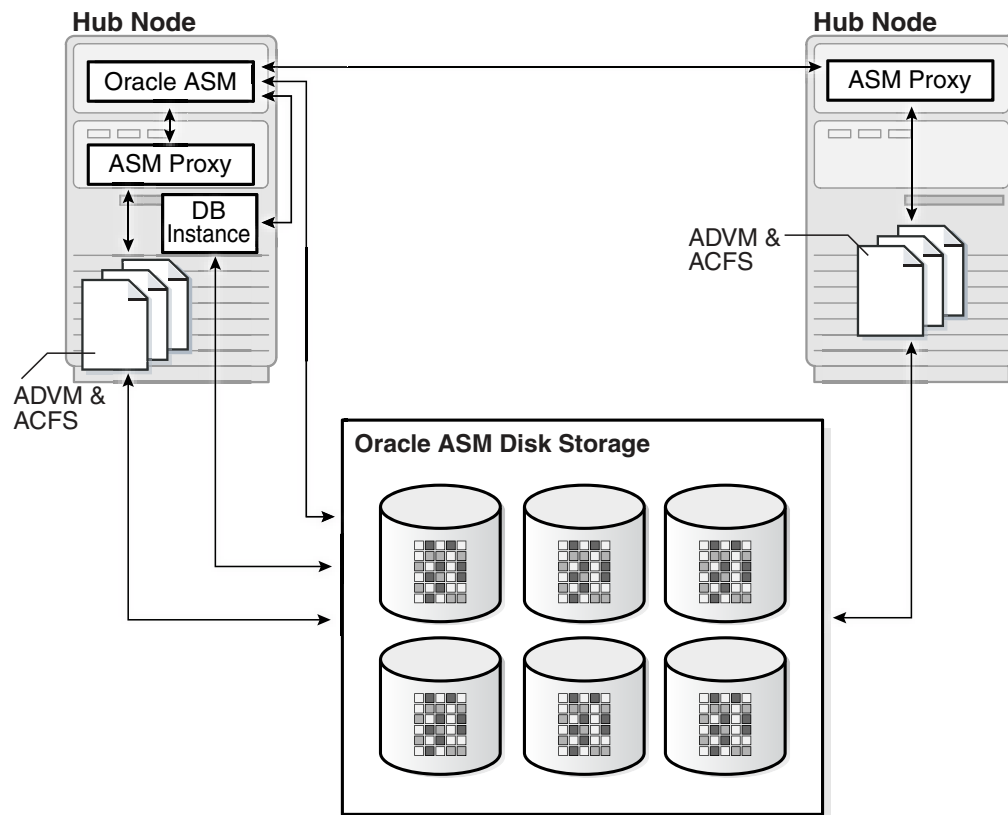
- Oracle ACFS access through the Oracle ASM proxy instance

An Oracle ASM proxy instance is an Oracle instance running on a Hub node with a direct Oracle ASM client. Oracle Automatic Storage Management Cluster File System (Oracle ACFS) and Oracle ASM Dynamic Volume Manager (Oracle ADVM) are supported with an Oracle ASM proxy instance. This configuration is shown in [Figure 2](#).

The `INSTANCE_TYPE` initialization parameter is set to `ASMPROXY` for Oracle ASM proxy instances.

Figure 2 shows the configuration of Oracle ACFS and Oracle ADVM in Oracle Flex ASM.

Figure 2 Oracle ACFS and Oracle ADVM in Oracle Flex ASM



About Setting Up Oracle Flex ASM

During the installation process with Oracle Universal Installer (OUI), you can choose the type of the Oracle Clusterware that should be installed. The Oracle Clusterware can be an Oracle Flex ASM deployment that manages its own storage or a regular Oracle ASM cluster.

Note:

- If you choose to install an Oracle Flex Cluster, Oracle Flex ASM is enabled by default because an Oracle Flex Cluster requires Oracle Flex ASM.
- Clients based on releases before Oracle Database 12c Release 1 (12.1) require the local Oracle ASM clients configuration described in [“Overview of Oracle Flex ASM”](#) or an Oracle Flex ASM configuration with the Oracle ASM instance count (cardinality) set to ALL.

For information about administering Oracle Flex ASM with SRVCTL commands, refer to [“Administering Oracle Flex ASM”](#).

- Oracle does not support changing Oracle Flex ASM to a standard Oracle ASM configuration.
-

To install an Oracle Flex ASM deployment, note the following:

- Categorize the networks and choose the list of networks for use as Oracle ASM networks.

If you choose Oracle Flex ASM during a new installation, OUI requires you to choose the Oracle ASM networks.

The Oracle ASM listener resource is automatically created for each Oracle ASM network and then started on all nodes.

- Enable Oracle Flex ASM if necessary.

Run Oracle ASM Configuration Assistant (ASMCA) to enable Oracle Flex ASM in a standard Oracle ASM cluster. This functionality is only available in an Oracle Grid Infrastructure configuration, not an Oracle Restart configuration. For information about converting to Oracle Flex ASM, refer to [“About Converting to Oracle Flex ASM”](#).

To determine whether an Oracle Flex ASM has been enabled, use the ASMCMD `showclustermode` command. For information about `showclustermode`, refer to [“showclustermode”](#).

The ASMCA GUI utility steps through the requirements and changes all dependencies as required, including dependencies on Oracle ACFS. ASMCA informs you if additional tasks, such as moving a server parameter file (SPFILE) or password file (ORAPWD file) to a disk group, are required before the conversion. For information about those tasks, refer to [“About Backing Up_ Copying_ and Moving an Oracle ASM Initialization Parameter File”](#) and [“Managing a Shared Password File in a Disk Group”](#).

See Also:

Oracle Grid Infrastructure Installation Guide for information about Oracle Clusterware installation

Administering Oracle Flex ASM

Oracle Flex ASM is managed by ASMCA, CRSCTL, SQL*Plus, and SRVCTL. The `INSTANCE_TYPE` initialization parameter specifies the type of instance.

The `INSTANCE_TYPE` initialization parameter has an additional value `ASMPROXY`, in addition to `ASM` and `RDBMS`, to identify Oracle ASM proxy instances. An Oracle ASM proxy instance has its parameter set to `ASMPROXY`.

You can use the ASMCMD `showclustermode` command to determine whether Oracle Flex ASM is enabled. For example:

```
$ asmcmd showclustermode
ASM cluster : Flex mode enabled
```

SRVCTL is extended to enable an administrator to create or change attributes of Oracle Clusterware resources. You can use SRVCTL to determine the status of the instances in an Oracle Flex ASM configuration. For example:

```
$ srvctl status asm -detail
ASM is running on mynoden02,mynoden01
ASM is enabled.
```

You can also use SRVCTL to determine whether Oracle Flex ASM is enabled. If enabled, then `srvctl config asm` displays the number of Oracle ASM instances that has been specified for use with the Oracle Flex ASM configuration. For example:

```
$ srvctl config asm
ASM instance count: 3
```

You can modify the Oracle ASM instance count, or cardinality, with the SRVCTL `modify asm` command. For example:

```
$ srvctl modify asm -count 4

$ srvctl modify asm -count ALL
```

You can view Oracle Flex ASM connections with SQL*Plus and ASMCMD commands. For example:

```
SQL> SELECT instance_name, db_name, status FROM V$ASM_CLIENT;
INSTANCE_NAME  DB_NAME  STATUS
-----
+ASM1          +ASM     CONNECTED
orcl1          orcl     CONNECTED
orcl2          orcl     CONNECTED

$ asmcmd lsct data
DB_Name  Status      Software_Version  Compatible_version  Instance_Name
Disk_Group
+ASM     CONNECTED   12.1.0.0.2        12.1.0.0.2        +ASM          DATA
orcl1    CONNECTED   12.1.0.0.2        12.0.0.0.0        orcl1         DATA
orcl1    CONNECTED   12.1.0.0.2        12.0.0.0.0        orcl2         DATA
```

Clients are automatically relocated to another instance if an Oracle ASM instance fails. If necessary, clients can be manually relocated using the `ALTER SYSTEM RELOCATE CLIENT` command. For example:

```
SQL> ALTER SYSTEM RELOCATE CLIENT 'client-id';
```

In the previous SQL statement, `client-id` is of the form `instance_name:db_name`. The `INSTANCE_NAME` and `DB_NAME` columns are contained in the `V$ASM_CLIENT` view. You must connect as `SYSASM` to the Oracle ASM instance to run the SQL statement. When you issue this statement, the connection to the client is terminated and the client fails over to the least loaded instance. If the client is currently connected to the least loaded instance, then the connection to the client is terminated and the client fails over to that same instance.

Every database user must have a wallet with credentials to connect to Oracle ASM. `CRSCTL` commands can be used by the database user to manage this wallet. All Oracle ASM user names and passwords are system generated.

There are no new initialization parameters specifically for instances in an Oracle Flex ASM configuration; however, the settings of existing parameters should be reviewed and possibly adjusted for the Oracle Flex ASM environment. Refer to [“Recommended Settings for Oracle ASM Initialization Parameters”](#).

See Also:

- *Oracle Database Reference* for more information about the `INSTANCE_TYPE` initialization parameter
 - *Oracle Database SQL Language Reference* for information about the `ALTER SYSTEM` statement
 - *Oracle Clusterware Administration and Deployment Guide* for information about `CRSCTL` commands
 - *Oracle Real Application Clusters Administration and Deployment Guide* for information about `SRVCTL` commands
 - *Oracle Grid Infrastructure Installation Guide* for information about installing Oracle Clusterware
-
-

Using Oracle Restart

Oracle Restart improves the availability of your Oracle Database. When you install the Oracle Grid Infrastructure for a standalone server, it includes both Oracle ASM and Oracle Restart. Oracle Restart runs out of the Oracle Grid Infrastructure home, which you install separately from Oracle Database homes.

Oracle Restart provides managed startup and restart of a single-instance (non-clustered) Oracle Database, Oracle ASM instance, service, listener, and any other process running on the server. If an interruption of a service occurs after a hardware or software failure, Oracle Restart automatically takes the necessary steps to restart the component.

With Server Control Utility (SRVCTL) you can add a component, such as an Oracle ASM instance, to Oracle Restart. You then enable Oracle Restart protection for the Oracle ASM instance. With SRVCTL, you also remove or disable Oracle Restart protection.

See Also:

- *Oracle Database Administrator's Guide* for information about configuring and administering Oracle Restart
 - *Oracle Real Application Clusters Administration and Deployment Guide* for information about automatically restarting single-instance databases residing on an Oracle RAC node
 - *Oracle Grid Infrastructure Installation Guide* for information about installation of Oracle Grid Infrastructure
-
-

About Starting Up an Oracle ASM Instance

This section describes how to start Oracle ASM instances under the following topics:

- [Connecting To and Starting Up an Oracle ASM Instance](#)
- [Starting Up an Oracle ASM instance with an Incorrect SPFILE Path](#)

- [About Mounting Disk Groups at Startup](#)
- [About Restricted Mode](#)

Connecting To and Starting Up an Oracle ASM Instance

You start an Oracle ASM instance similarly to the way in which you start an Oracle Database instance with some minor differences.

When starting an Oracle ASM instance, note the following:

- To connect to a local Oracle ASM instance with SQL*Plus, set the `ORACLE_SID` environment variable to the Oracle ASM system identifier (SID).

The default Oracle ASM SID for a single-instance database is `+ASM`, and the default SID for Oracle ASM for an Oracle RAC node is `+ASMnode_number` where `node_number` is the number of the node. The `ORACLE_HOME` environment variable must be set to the Grid Infrastructure home where Oracle ASM was installed.

Note:

Oracle recommends that you do not change the default Oracle ASM SID name.

- The initialization parameter file must contain the following entry:

```
INSTANCE_TYPE = ASM
```

This parameter indicates that an Oracle ASM instance, not a database instance, is starting.

- When you run the `STARTUP` command, rather than trying to mount and open a database, this command attempts to mount Oracle ASM disk groups.

For information about disk groups that are mounted at startup time, see [“About Mounting Disk Groups at Startup”](#).

After the Oracle ASM instance has started, you can mount disk groups with the `ALTER DISKGROUP . . . MOUNT` command. See [“Mounting and Dismounting Disk Groups”](#) for more information.

- The associated Oracle Database instance does not have to be running when you start the associated Oracle ASM instance.

The following list describes how Oracle ASM interprets SQL*Plus `STARTUP` command parameters.

- **FORCE Parameter**

Issues a `SHUTDOWN ABORT` to the Oracle ASM instance before restarting it.

If an Oracle Automatic Storage Management Cluster File System (Oracle ACFS) file system is currently mounted on Oracle ADVM volumes, the file system should first be dismounted. Otherwise, applications encounter I/O errors and Oracle ACFS user data and metadata may not be written to storage before the Oracle ASM storage is fenced. For information about dismounting an Oracle ACFS file system, see [“Deregistering_ Dismounting_ and Disabling Volumes and Oracle ACFS File Systems”](#).

- MOUNT or OPEN Parameter

Mounts the disk groups specified in the `ASM_DISKGROUPS` initialization parameter. This is the default if no command parameter is specified.

- NOMOUNT Parameter

Starts up the Oracle ASM instance without mounting any disk groups.

- RESTRICT Parameter

Starts up an instance in restricted mode that enables access only to users with both the `CREATE SESSION` and `RESTRICTED SESSION` system privileges. You can use the `RESTRICT` clause in combination with the `MOUNT`, `NOMOUNT`, and `OPEN` clauses.

See Also:

[“About Restricted Mode”](#) for more information

In restricted mode, database instances cannot use the disk groups. In other words, databases cannot open files that are in that disk group. Also, the disk group cannot be mounted by any other instance in the cluster. Mounting the disk group in restricted mode enables only one Oracle ASM instance to mount the disk group. This mode is useful to mount the disk group for repairing configuration issues.

The following is a sample SQL*Plus session for starting an Oracle ASM instance.

```
SQLPLUS /NOLOG
SQL> CONNECT SYS AS SYSASM
Enter password: sys_password
Connected to an idle instance.

SQL> STARTUP
ASM instance started

Total System Global Area      71303168 bytes
Fixed Size                    1069292 bytes
Variable Size                  45068052 bytes
ASM Cache                      25165824 bytes
ASM disk groups mounted
```

For more information about user authentication, see [“Authentication for Accessing Oracle ASM Instances”](#).

See Also:

- *Oracle Database Administrator's Guide* for more information about using environment variables to select instances
 - *Oracle Database Administrator's Guide* for more information about starting up and shutting down Oracle instances
 - *Oracle Real Application Clusters Administration and Deployment Guide* for information about starting an Oracle ASM instance with `SRVCTL` in Oracle RAC
 - *Oracle Clusterware Administration and Deployment Guide* for information about Oracle Clusterware Cluster subcomponent processes and background processes
 - *Oracle Database Concepts* for information about Oracle Database background processes
 - *Oracle Database Reference* for a description of the Oracle background processes
-

Starting Up an Oracle ASM instance with an Incorrect SPFILE Path

If the SPFILE path in the GPnP profile is incorrect, you can start the Oracle ASM instance as follows:

1. Create a PFILE with one line in it that identifies the path to the SPFILE.

For example:

Create the `/oracle/dbs/spfileasm_init.ora` file that contains:

```
SPFILE= '+DATA/asm/asmparameterfile/asmspfile.ora'
```

2. Start up the instance using the initialization parameter file.

For example:

```
SQL> STARTUP PFILE=/oracle/dbs/spfileasm_init.ora
```

3. After the instance is running, use the `ASMCMD spset` command to update the SPFILE path in the GPnP profile. See "[spset](#)".

For example:

```
ASMCMD> spset +DATA/asm/asmparameterfile/asmspfile.ora
```

See Also:

Oracle Database Administrator's Guide for more information about using `STARTUP` with a nondefault server parameter file

About Mounting Disk Groups at Startup

At startup, the Oracle ASM instance attempts to mount the following disk groups:

- Disk groups specified in the `ASM_DISKGROUPS` initialization parameter
- Disk group used by Cluster Synchronization Services (CSS) for voting files
- Disk groups used by Oracle Clusterware for Oracle Cluster Registry (OCR)
- Disk group used by the Oracle ASM instance to store the ASM server parameter file (SPFILE)

If no disk groups are found in the previous list, then the Oracle ASM instance does not mount any disk groups at startup. After the Oracle ASM instance has started, you can mount disk groups with the `ALTER DISKGROUP . . . MOUNT` command. For more information, see [“Mounting and Dismounting Disk Groups”](#).

About Restricted Mode

You can use the `STARTUP RESTRICT` command to control access to an Oracle ASM instance while you perform maintenance. When an Oracle ASM instance is active in this mode, all of the disk groups that are defined in the `ASM_DISKGROUPS` parameter are mounted in `RESTRICTED` mode. This prevents databases from connecting to the Oracle ASM instance. In addition, the restricted clause of the `ALTER SYSTEM` statement is disabled for the Oracle ASM instance. The `ALTER DISKGROUP diskgroup MOUNT` statement is extended to enable Oracle ASM to mount a disk group in restricted mode.

When you mount a disk group in `RESTRICTED` mode, the disk group can only be mounted by one instance. Clients of Oracle ASM on that node cannot access that disk group while the disk group is mounted in `RESTRICTED` mode. The `RESTRICTED` mode enables you to perform maintenance tasks on a disk group in the Oracle ASM instance without interference from clients.

Rebalance operations that occur while a disk group is in `RESTRICTED` mode eliminate the lock and unlock extent map messaging that occurs between Oracle ASM instances in an Oracle RAC environment. This improves the overall rebalance throughput. At the end of a maintenance period, you must explicitly dismount the disk group and remount it in normal mode.

About Shutting Down an Oracle ASM Instance

The Oracle ASM shutdown process is initiated when you run the `SHUTDOWN` command in SQL*Plus. Before you run this command, ensure that the `ORACLE_SID` environment variable is set to the Oracle ASM SID so that you can connect to the local Oracle ASM instance. The default Oracle ASM SID for a single-instance database is `+ASM`, and the default SID for Oracle ASM for an Oracle RAC node is `+ASMnode_number` where `node_number` is the number of the node. The `ORACLE_HOME` environment variable must be set to the Grid Infrastructure home where Oracle ASM was installed.

If you are not using Oracle Flex ASM, Oracle strongly recommends that you shut down all database instances that use the Oracle ASM instance and dismount all file systems mounted on Oracle ASM Dynamic Volume Manager (Oracle ADVM) volumes before attempting to shut down the Oracle ASM instance. If you are using Oracle Flex ASM, Oracle Flex ASM clients move to other running Oracle ASM instances if an Oracle ASM instance is shut down.

If Oracle Cluster Registry (OCR) or voting files are stored in a disk group, the disk group can only be dismounted by shutting down the Oracle ASM instance as part of shutting down the clusterware on a node. To shut down the clusterware, run `crsctl stop crs`.

See Also:

- *Oracle Database Administrator's Guide* for more information about using environment variables to select instances
 - *Oracle Database Administrator's Guide* for more information about starting up and shutting down Oracle instances
 - *Oracle Clusterware Administration and Deployment Guide* for information about managing voting files, Oracle Cluster Registry (OCR), and Oracle Local Registry (OLR)
-

To shut down an Oracle ASM instance, perform the following steps:

```
SQLPLUS /NOLOG
SQL> CONNECT SYS AS SYSASM
Enter password: sys_password
Connected.
SQL> SHUTDOWN NORMAL
```

For more information about user authentication, see [“Authentication for Accessing Oracle ASM Instances”](#).

The following list describes the SHUTDOWN modes and the behavior of the Oracle ASM instance in each mode.

- **NORMAL** Clause
Oracle ASM waits for any in-progress SQL to complete before performing an orderly dismount of all of the disk groups and shutting down the Oracle ASM instance. Before the instance is shut down, Oracle ASM waits for all of the currently connected users to disconnect from the instance. If any database instances are connected to the Oracle ASM instance, then the SHUTDOWN command returns an error and leaves the Oracle ASM instance running. NORMAL is the default shutdown mode.
- **IMMEDIATE** or **TRANSACTIONAL** Clause
Oracle ASM waits for any in-progress SQL to complete before performing an orderly dismount of all of the disk groups and shutting down the Oracle ASM instance. Oracle ASM does not wait for users currently connected to the instance to disconnect. If any database instances are connected to the Oracle ASM instance, then the SHUTDOWN command returns an error and leaves the Oracle ASM instance running. Because the Oracle ASM instance does not contain any transactions, the TRANSACTIONAL mode behaves the same as IMMEDIATE mode.
- **ABORT** Clause
The Oracle ASM instance immediately shuts down without the orderly dismount of disk groups. This causes recovery to occur upon the next Oracle ASM startup.
If any database instance is connected to the Oracle ASM instance, then the database instance aborts.
If any Oracle Automatic Storage Management Cluster File System (Oracle ACFS) file systems are currently mounted on Oracle ADVM volumes, those file systems should first be dismounted. Otherwise, applications encounter I/O errors and Oracle ACFS user data and metadata may not be written to storage before the Oracle ASM storage is fenced. For information about dismounting an Oracle ACFS

file system, see [“Deregistering_ Dismounting_ and Disabling Volumes and Oracle ACFS File Systems”](#). For more information about user authentication on Oracle ASM instance, see [“Authentication for Accessing Oracle ASM Instances”](#).

About Administering Oracle ASM Instances with Server Control Utility

In addition to the Oracle ASM administration procedures that this section describes, you can use Server Control Utility (SRVCTL) in clustered Oracle ASM environments to perform the following Oracle ASM administration tasks:

- Add and remove the Oracle ASM Oracle Clusterware (CRS) resource in Oracle Cluster Registry (OCR)
- Enable, disable, start, and stop Oracle ASM instances
- Display the Oracle ASM instance configuration and status

See Also:

The *Oracle Real Application Clusters Administration and Deployment Guide* for information about administering Oracle ASM instances with SRVCTL

About Out of Place Upgrades

With an out-of-place upgrade, the installer installs the newer version of Oracle Grid Infrastructure in a separate Oracle Grid Infrastructure home.

An in-place upgrade of Oracle Grid Infrastructure 11g Release 2 (11.2) is not supported. For example, an upgrade of Oracle Grid Infrastructure 11g Release 2 (11.2.0.1) to Oracle Grid Infrastructure 11g Release 2 (11.2.0.2) must be an out of place upgrade.

See Also:

Oracle Grid Infrastructure Installation Guide for information about installing Oracle Grid Infrastructure, out of place upgrades, and performing rolling upgrades of Oracle Grid Infrastructure and Oracle ASM

About Configuring Oracle Grid Infrastructure with the Configuration Wizard

The Oracle Grid Infrastructure configuration wizard can update the configuration of an Oracle Grid Infrastructure environment after the software has been installed. The configuration wizard accepts your input, validates the input, and populates the configuration data into the `CRSCONFIG_PARAMS` file. If additional scripts must be run, the configuration wizard directs you to run those scripts.

See Also:

Oracle Clusterware Administration and Deployment Guide for information about the Oracle Grid Infrastructure configuration wizard.

About Active Session History Sampling for Oracle ASM

Active Session History sampling is now available on Oracle ASM instances. This activity is exposed in the dynamic `V$ACTIVE_SESSION_HISTORY` view. Active Session History sampling requires a diagnostic pack license for the Oracle ASM instance.

See Also:

- *Oracle Database Performance Tuning Guide* for more information about gathering performance statistics
 - *Oracle Database Reference* for a description of the `V$ACTIVE_SESSION_HISTORY` view
-
-

About Oracle Home User on Windows

Oracle Database supports the use of an Oracle home user, which can be specified at installation time. The Oracle home user is associated with an Oracle home and it cannot be changed after installation. Different Oracle homes on a system can share the same Oracle home user or use different Oracle home user names.

In previous releases on Windows operating systems, Oracle services were required to run as `Local System` privileges, which are fully privileged. This feature enables the database, listener, and job scheduler services to run with low and non-administrative user privileges to allow tighter control of security. The Oracle home user can be a built-in account or a Windows user account. A Windows user account should be a low privileged (non-Administrator) account to ensure that the Oracle home user has a limited set of privileges, ensuring that Oracle Database services have only those privileges required to run Oracle products. The Windows user account can be a Local User, a Domain User, or a Managed Services Account in general. However, Oracle RAC, Oracle Restart, and Oracle Grid Infrastructure installations require the use of the Domain User as the Oracle home user because a clusterwide identity is necessary.

See Also:

Oracle Database Platform Guide for Microsoft Windows for information about running Oracle services on Windows platforms and different types of Windows user accounts

Upgrading and Patching Oracle ASM

This section contains the following topics:

- [About Oracle ASM Rolling Upgrade](#)
- [About Oracle ASM Rolling Patches](#)
- [About Converting to Oracle Flex ASM](#)

Note:

- For Oracle RAC environments, the Oracle Clusterware version number must be at least equal to the version number of the patch that you are applying to the Oracle Database.
 - You must apply the patch to the Oracle Grid Infrastructure home before you apply it to the Oracle Database home.
-

About Oracle ASM Rolling Upgrade

Oracle ASM rolling upgrade enables you to independently upgrade or patch clustered Oracle ASM nodes without affecting database availability, thus providing greater uptime. Rolling upgrade means that some features of a clustered Oracle ASM environment continue to function when one or more of the nodes in the cluster uses different software versions. Oracle recommends that you perform an Oracle ASM rolling upgrade when performing an Oracle Clusterware rolling upgrade.

To perform a rolling upgrade, your environment must be prepared. Oracle Clusterware must be fully upgraded to the next patch or release version before you start the Oracle ASM rolling upgrade. In addition, you should prepare your Oracle Clusterware in a rolling upgrade manner to ensure high availability and maximum uptime.

Note that Oracle ASM is upgraded with Oracle Clusterware for Oracle 11g Release 2 (11.2) or later as both are in the Oracle Grid Infrastructure home.

Note:

- Rolling upgrades only apply to clustered Oracle ASM instances, and you can only perform rolling upgrades on environments with Oracle Database 11g or later. You cannot use this feature to upgrade from Oracle Database 10g to Oracle Database 11g.
 - See *Oracle Exadata documentation* for information about performing a rolling upgrading of an Oracle ASM instance when Oracle Exadata storage is present.
-

See Also:

- *Oracle Grid Infrastructure Installation Guide* for information about performing, and restrictions related to, a rolling upgrade of Oracle ASM
 - *Oracle Database Upgrade Guide* for information about upgrading Oracle Database
 - *Oracle Database SQL Language Reference* for information about the rolling migration clause of the ALTER SYSTEM command
-

About Oracle ASM Rolling Patches

You can apply patches in a clustered Oracle ASM environment to update one node at a time to the latest patch level without affecting the overall availability of the Oracle ASM cluster or the database clusters using Oracle ASM for storage.

The `ALTER SYSTEM ROLLING PATCH` SQL statement enables you to start and stop rolling patches. For example:

```
SQL> ALTER SYSTEM START ROLLING PATCH;
```

```
SQL> ALTER SYSTEM STOP ROLLING PATCH;
```

You can determine if the cluster is in rolling patch mode by executing a `SYS_CONTEXT` SQL query for Cluster State. A new state (In Rolling Patch) is added to informing the user that the cluster is in rolling patch mode.

The queries in [Example 2](#) display information about rolling patches. To run these queries, you must be connected to the Oracle ASM instance in the Grid home, and the Grid Infrastructure home must be configured with the Oracle Clusterware option for an Oracle RAC environment.

You can view all the patch Ids applied on the node and cluster by querying the `V$PATCHES` view.

ASMCMD commands for rolling patches include:

- `showclusterstate`
- `showpatches`
- `showversion`

For information about ASMCMD commands to monitor upgrade operations on an Oracle ASM instance, refer to “[ASMCMD Instance Management Commands](#)”.

See Also:

- *Oracle Database SQL Language Reference* for information about the rolling patch clause of the `ALTER SYSTEM` command
 - *Oracle Grid Infrastructure Installation Guide* for information about performing, and restrictions related to, a rolling migration of Oracle ASM and Oracle Grid Infrastructure homes
-
-

Example 2 Determining rolling patch mode and patch level

```
SELECT SYS_CONTEXT('SYS_CLUSTER_PROPERTIES', 'CLUSTER_STATE') FROM DUAL;
```

```
SELECT SYS_CONTEXT('SYS_CLUSTER_PROPERTIES', 'CURRENT_PATCHLVL') FROM DUAL;
```

About Converting to Oracle Flex ASM

You can convert an Oracle ASM configuration to an Oracle Flex ASM using ASMCA. This functionality is only available in an Oracle Grid Infrastructure 12c configuration. For information about using ASMCA, refer to “[Getting Started With the ASMCA GUI Tool](#)”. For

Note:

- If you plan to introduce databases before Oracle Database 12c Release 1 (12.1) into a cluster configured with Oracle Flex ASM, you must ensure that Oracle ASM instances are running on all nodes in the cluster, including nodes that are added in the future. To ensure this requirement for the Oracle Flex ASM configuration, you must set the count of Oracle ASM instances to ALL with the `SRVCTL modify asm` command. For information about administering Oracle Flex ASM with SRVCTL commands, refer to [“Administering Oracle Flex ASM”](#).
 - For additional considerations, refer to the **Notes** in [“About Setting Up Oracle Flex ASM”](#).
-

Before you convert an Oracle ASM configuration to an Oracle Flex ASM, you must ensure the following:

- Oracle Cluster Registry (OCR) is stored in a disk group. For information about storing OCR in a disk group, refer to [“Storing Oracle Cluster Registry and Voting Files in Oracle ASM Disk Groups”](#).
-

See Also:

Oracle Clusterware Administration and Deployment Guide for information about managing Oracle Cluster Registry and Oracle Local Registry

- The server parameter file (SPFILE) is stored in a disk group. For information about storing an SPFILE file in a disk group, refer to [“About Backing Up_ Copying_ and Moving an Oracle ASM Initialization Parameter File”](#).
- The password file (ORAPWD file) is stored in a disk group. For information about storing an ORAPWD file in a disk group, refer to [“Managing a Shared Password File in a Disk Group”](#).
- The disk group where the OCR, SPFILE, and ORAPWD files are stored has Oracle ASM compatibility (`COMPATIBLE.ASM`) set to 12.1 or higher. For information about disk group compatibility, refer to [“Disk Group Compatibility”](#).

ASMCA informs you if any requirement, such as storing an ORAPWD file in a disk group, has not been met before starting the conversion.

[Figure 3](#) shows the **Configure ASM: ASM Instances** page that enables you to perform operations on selected Oracle ASM instances.

Figure 3 Oracle ASM Configuration Assistant Configure ASM Instances Page

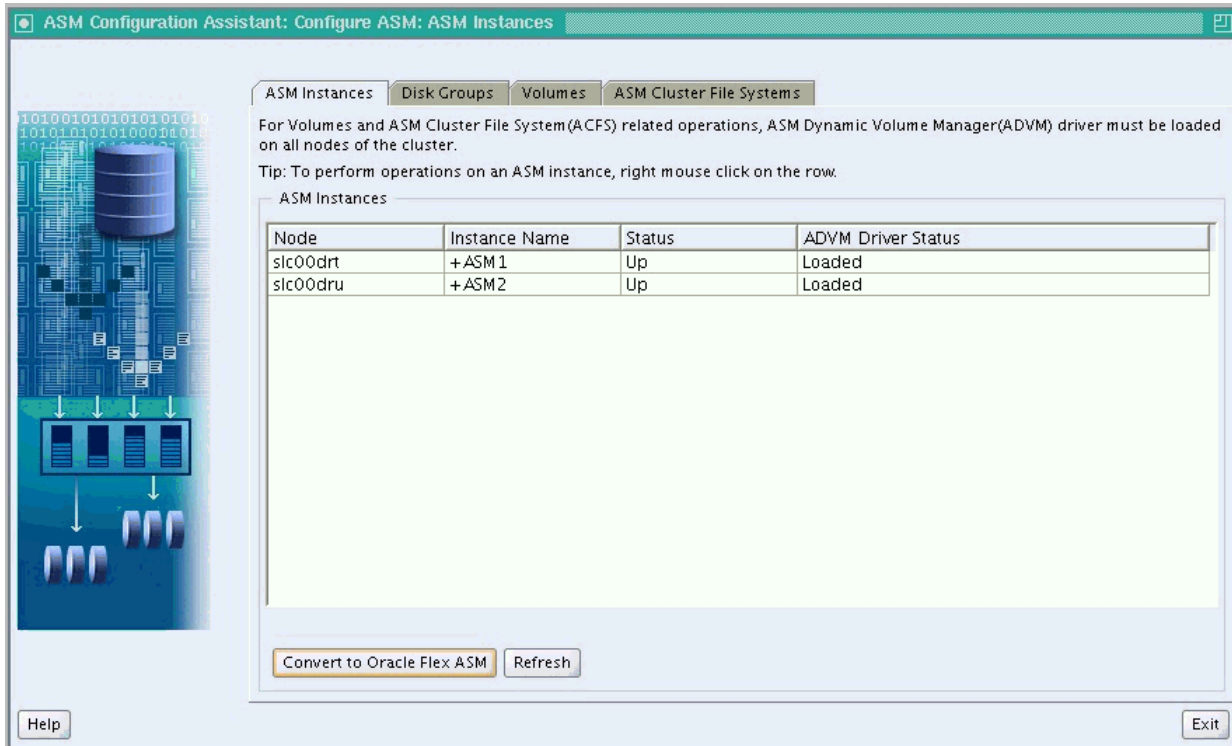
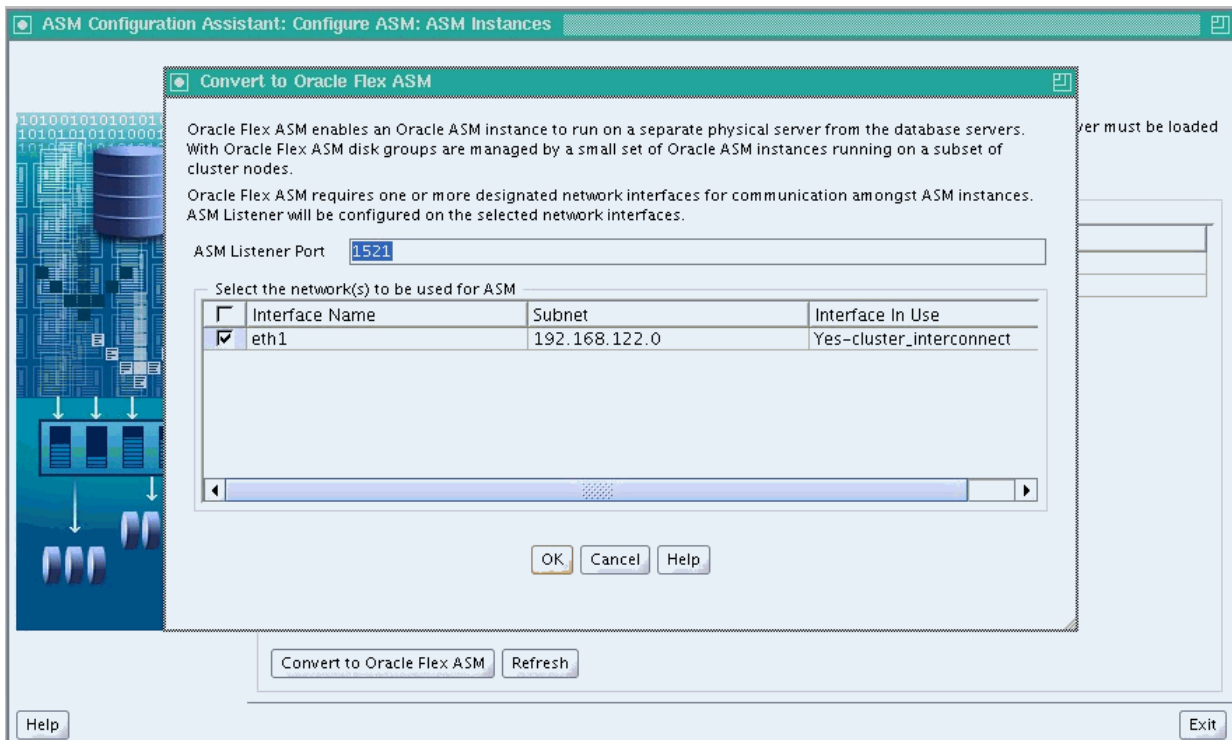


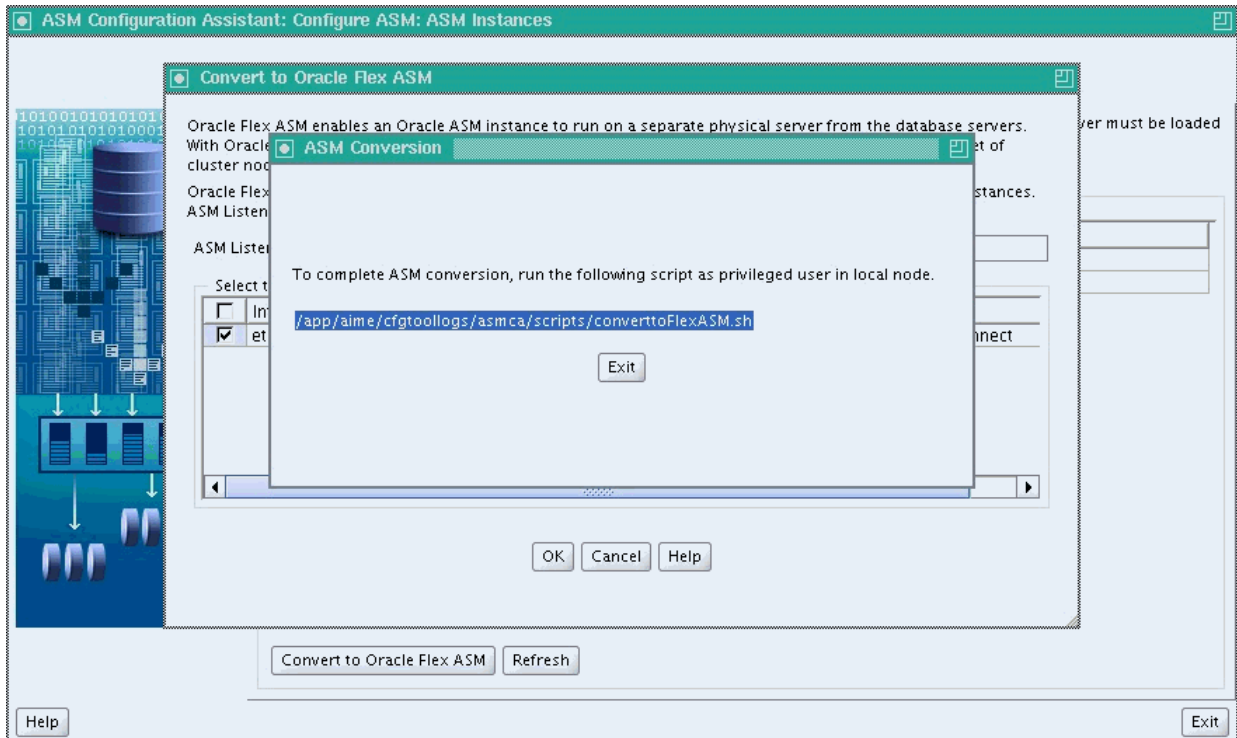
Figure 4 shows the Convert to Oracle Flex ASM dialog box that enables you to specify the listener port and network interface for the conversion to Oracle Flex ASM.

Figure 4 Oracle ASM Configuration Assistant Convert to Oracle Flex ASM Dialog Box



To complete the Oracle Flex ASM conversion, ASMCA generates the `converttoFlexASM.sh` script that must be run as privileged user only on the local node where ASMCA is running. [Figure 5](#) shows the **ASM Conversion** dialog box with the script that must be run.

Figure 5 Oracle ASM Configuration Assistant ASM Conversion Dialog Box



For information about the ASMCA command-line option for converting to Oracle Flex ASM, refer to [“Convert to Oracle Flex ASM”](#).

For information about Oracle Flex ASM, refer to [“Managing Oracle Flex ASM”](#).

See Also:

Oracle Grid Infrastructure Installation Guide for information about installing and upgrading Oracle Grid Infrastructure

Oracle ASM Filter Driver

Note:

This feature is available on Linux systems starting with Oracle Database 12c Release 1 (12.1.0.2).

Oracle ASM Filter Driver (Oracle ASMFDF) is a kernel module that resides in the I/O path of the Oracle ASM disks. After installation of Oracle Grid Infrastructure, you can optionally configure Oracle ASMFDF for your system. If ASMLIB is configured for an existing Oracle ASM installation, then you must explicitly migrate the existing ASMLIB configuration to Oracle ASMFDF.

Note:

In the steps of the procedures in this section, the `$ORACLE_HOME` environmental variable is set to the directory path of the Oracle Grid Infrastructure home. Commands that show `#` as the operating system prompt must be run as the root user. Commands that show `$` as the operating system prompt should be run as the owner of Oracle Grid Infrastructure home.

This section contains the following topics:

- [About Oracle ASM Filter Driver](#)
- [Deciding Between Oracle ASMLIB and Oracle ASM Filter Driver](#)
- [Configuring Oracle ASM Filter Driver](#)
- [About Migrating to Oracle ASM Filter Driver From ASMLIB](#)
- [Determining Whether Oracle ASM Filter Driver Has Been Configured](#)
- [Updating the Oracle ASM Filter Driver `AFD_DISKSTRING` Parameter](#)
- [Updating the Oracle ASM `ASM_DISKSTRING` Parameter for Oracle ASM Filter Driver Disks](#)
- [Setting_ Clearing_ and Scanning Oracle ASM Filter Driver Labels](#)
- [Deconfiguring Oracle ASM Filter Driver](#)

For information about the `ASMCMD` commands for administering Oracle ASMFD, refer to “[ASMCMD Oracle ASM Filter Driver Management Commands](#)”.

For information about all the `ASMCMD` commands, refer to “[About ASMCMD](#)”.

For information about using Oracle Enterprise Manager to administer Oracle ASMFD, refer to “[Managing Oracle ASM Filter Driver With Oracle Enterprise Manager](#)”.

See Also:

Oracle Grid Infrastructure Installation Guide for your operating system for information about installing and configuring Oracle Grid Infrastructure

About Oracle ASM Filter Driver

Oracle ASM Filter Driver (Oracle ASMFD) is a kernel module that resides in the I/O path of the Oracle ASM disks. Oracle ASM uses the filter driver to validate write I/O requests to Oracle ASM disks.

The Oracle ASMFD simplifies the configuration and management of disk devices by eliminating the need to rebind disk devices used with Oracle ASM each time the system is restarted.

The Oracle ASM Filter Driver rejects any I/O requests that are invalid. This action eliminates accidental overwrites of Oracle ASM disks that would cause corruption in the disks and files within the disk group. For example, the Oracle ASM Filter Driver filters out all non-Oracle I/Os which could cause accidental overwrites.

Deciding Between Oracle ASMLIB and Oracle ASM Filter Driver

Oracle ASM Filter Driver (Oracle ASMFD) is installed with an Oracle Grid Infrastructure installation. If you have an existing Oracle ASM library driver (Oracle ASMLIB) configuration, then depending on whether you want to use Oracle ASMLIB or Oracle ASMFD, consider the following scenarios:

- If you use Oracle ASMLIB to manage your Oracle ASM devices and you want to continue to use Oracle ASMLIB, then upgrade to Oracle Grid Infrastructure 12c Release 1 (12.1.0.2).

Although Oracle ASMFD is installed, Oracle ASMLIB continues to be used for device persistence.

- If you use Oracle ASMLIB to manage your Oracle ASM devices and you want to migrate to Oracle ASMFD, then perform the following steps:

1. Upgrade to Oracle Grid Infrastructure 12c Release 1 (12.1.0.2).

This process installs Oracle ASMFD.

2. Migrate from Oracle ASMLIB to Oracle ASMFD.

Refer to [“Configuring Oracle ASM Filter Driver”](#) to remove Oracle ASMLIB and configure your Oracle ASM devices to use Oracle ASMFD for device persistence.

- If Oracle ASMLIB is installed, but you do not use Oracle ASM because Oracle Grid Infrastructure is not installed, and want to use Oracle ASMFD, then follow these steps:

1. Deinstall Oracle ASMLIB.

See Also:

Oracle Grid Infrastructure Installation Guide for your operating system for information about installing and deinstalling Oracle ASMLIB

2. Install Oracle Grid Infrastructure 12c Release 1 (12.1.0.2).

This process installs Oracle ASMFD.

3. Configure your Oracle ASM devices to use Oracle ASMFD for device persistence.

Refer to [“Configuring Oracle ASM Filter Driver”](#).

4. Create disk labels to enable migration of Oracle ASM disk groups to Oracle ASMFD.

Refer to [“About Migrating to Oracle ASM Filter Driver From ASMLIB”](#).

You can also set udev rules, in addition to or instead of Oracle ASMFD and Oracle ASMLIB, for device persistence.

Configuring Oracle ASM Filter Driver

After installing Oracle Grid Infrastructure 12c Release 1 (12.1.0.2), you can configure your Oracle ASM devices to use Oracle ASM Filter Driver (ASMFd) for device persistence.

This section contains the following topics:

- [“Configuring Oracle ASM in an Oracle Grid Infrastructure Clusterware Environment”](#)
- [“Configuring Oracle ASM in an Oracle Grid Infrastructure Standalone \(Oracle Restart\) Environment”](#)

See Also:

Oracle Clusterware Administration and Deployment Guide for information about using CRSCTL commands

Configuring Oracle ASM in an Oracle Grid Infrastructure Clusterware Environment

To configure Oracle ASMFd in an Oracle Clusterware environment, follow these steps:

1. As the Oracle Grid Infrastructure owner update the Oracle ASM disk discovery string to enable Oracle ASMFd to discover devices in the future.

For example, check the current value of the Oracle ASM disk discovery string and then update the value.

```
$ $ORACLE_HOME/bin/asmcmd dsget
```

```
$ $ORACLE_HOME/bin/asmcmd dsset old_diskstring, 'AFD:*
```

The value of *old_diskstring* is the current Oracle ASM disk discovery string value.

For information about updating the Oracle ASM discovery string, refer to [“Updating the Oracle ASM ASM_DISKSTRING Parameter for Oracle ASM Filter Driver Disks”](#).

2. As the Oracle Grid Infrastructure owner list the nodes and node roles in your cluster:

```
$ $ORACLE_HOME/bin/olsnodes -a
```

3. On each Hub node, do the following, either in rolling or non-rolling mode:

- a. Log in as the `root` user and stop Oracle Grid Infrastructure:

```
# $ORACLE_HOME/bin/crsctl stop crs
```

If the command returns an error, then stop Oracle Grid Infrastructure forcibly as follows:

```
# $ORACLE_HOME/bin/crsctl stop crs -f
```

- b. As `root`, configure Oracle ASMFd to filter at the node level:

```
# $ORACLE_HOME/bin/asmcmd afd_configure
```

- c. As the Oracle Grid Infrastructure owner verify the status of Oracle ASMFD:

```
$ $ORACLE_HOME/bin/asmcmd afd_state
ASMCMD-9526: The AFD state is 'LOADED' and filtering is 'ENABLED' on
host 'myhost'
```

For information about checking on the state of the Oracle ASM Filter Driver, refer to [“Determining Whether Oracle ASM Filter Driver Has Been Configured”](#).

- d. As root, start the Oracle Clusterware stack on the node:

```
# $ORACLE_HOME/bin/crsctl start crs
```

- e. As the Oracle Grid Infrastructure owner set the Oracle ASMFD discovery disk string to the original Oracle ASM disk discovery string value that was retrieved in Step 1:

```
$ $ORACLE_HOME/bin/asmcmd afd_dsset old_diskstring
```

The value of *old_diskstring* is the old disk discovery string value without the AFD: (Oracle ASMFD) path.

For information about updating the Oracle ASM Filter Driver discovery disk discovery string, refer to [“Updating the Oracle ASM Filter Driver AFD_DISKSTRING Parameter”](#).

For information about updating the Oracle ASM discovery disk discovery string, refer to [“Updating the Oracle ASM ASM_DISKSTRING Parameter for Oracle ASM Filter Driver Disks”](#).

Oracle ASM Filter Driver should identify and start managing disks previously managed by Oracle ASMLIB.

Configuring Oracle ASM in an Oracle Grid Infrastructure Standalone (Oracle Restart) Environment

To configure Oracle ASMFD in a standalone environment, follow these steps:

1. As the Oracle Grid Infrastructure standalone server owner update the Oracle ASM disk discovery string to enable Oracle ASMFD to discover disk devices.

For example, check the current value of the Oracle ASM disk discovery string and then update the value.

```
$ $ORACLE_HOME/bin/asmcmd dsget
$ $ORACLE_HOME/bin/asmcmd dsset old_diskstring, 'AFD:*
```

Where *old_diskstring* is the current disk discovery string value.

For information about updating the Oracle ASM discovery string, refer to [“Updating the Oracle ASM ASM_DISKSTRING Parameter for Oracle ASM Filter Driver Disks”](#).

2. Log in as the root user and stop Oracle Grid Infrastructure for a standalone server using the following command:

```
# $ORACLE_HOME/bin/crsctl stop has -f
```

3. As root, configure Oracle ASMFD using the following command:

```
# $ORACLE_HOME/bin/asmcmd afd_configure
```

This command configures Oracle ASMFD and deconfigures Oracle ASMLIB, if it exists.

4. As the Oracle Grid Infrastructure standalone server owner verify the Oracle ASMFD status:

```
$ $ORACLE_HOME/bin/asmcmd afd_state
```

```
ASMCMD-9526: The AFD state is 'LOADED' and filtering is 'ENABLED' on host 'myhost'
```

For information about checking on the state of the Oracle ASM Filter Driver, refer to [“Determining Whether Oracle ASM Filter Driver Has Been Configured”](#).

5. As root, start Oracle Grid Infrastructure for a standalone server:

```
# $ORACLE_HOME/bin/crsctl start has
```

6. As the Oracle Grid Infrastructure standalone server owner set the Oracle ASMFD disk discovery string to the original value of the Oracle ASM disk discovery string that was retrieved in Step 1:

```
$ $ORACLE_HOME/bin/asmcmd afd_dsset disk_string
```

Oracle ASM Filter Driver should identify and start managing disks previously managed by Oracle ASMLIB.

About Migrating to Oracle ASM Filter Driver From ASMLIB

If Oracle ASMLIB was installed, but not used earlier, you must create disk labels to enable migration of Oracle ASM disk groups to Oracle ASM Filter Driver (Oracle ASMFD) after installing Oracle Grid Infrastructure 12c Release 1 (12.1.0.2).

Oracle recommends that you temporarily move Oracle Cluster Registry (OCR) and voting files to another disk group if one is available, as described in [“Migrating Oracle ASM Disk Groups without Oracle Cluster Registry or Voting Files”](#), and migrate the disk group to use Oracle ASMFD. After migrating the disk group to use Oracle ASMFD, move OCR and voting files back to the disk group. You can similarly migrate any other disk groups if they contain OCR or voting files to ensure online migration of all disk groups to Oracle ASMFD.

This section contains the following topics:

- [“Migrating Oracle ASM Disk Groups without Oracle Cluster Registry or Voting Files”](#)
- [“Migrating Oracle ASM Disk Groups with Oracle Cluster Registry or Voting Files”](#)
- [“Migrating Oracle ASM Disk Groups in an Oracle Grid Infrastructure Standalone \(Oracle Restart\) Environment”](#)

See Also:

- *Oracle Clusterware Administration and Deployment Guide* for information about replacing Oracle Cluster Registry locations and migrating voting files
 - *Oracle Clusterware Administration and Deployment Guide* for information about using CRSCTL commands
 - *Oracle Clusterware Administration and Deployment Guide* for information about managing voting files, Oracle Cluster Registry (OCR), and Oracle Local Registry (OLR)
 - *Oracle Real Application Clusters Administration and Deployment Guide* for information about SRVCTL commands
-

Migrating Oracle ASM Disk Groups without Oracle Cluster Registry or Voting Files

To migrate Oracle ASM disk groups without Oracle Cluster Registry (OCR) or voting files to Oracle ASMFD:

1. Log in as the Oracle Grid Infrastructure owner on any node to run the commands in this procedure.

2. List the existing disk groups:

```
$ $ORACLE_HOME/bin/asmcmd lsdg
```

3. List the associated disks:

```
$ $ORACLE_HOME/bin/asmcmd lsdsk -G diskgroup
```

4. Check if Oracle ASM is active:

```
$ $ORACLE_HOME/bin/srvctl status asm
```

5. Stop the databases and dismount the disk group on all nodes:

```
$ $ORACLE_HOME/bin/srvctl stop diskgroup -diskgroup diskgroup -f
```

6. Label all existing disks in the disk group by running the following command for each disk on a Hub node:

```
$ $ORACLE_HOME/bin/asmcmd afd_label label disk_path --migrate
```

7. Scan the disks on all Hub nodes:

```
$ $ORACLE_HOME/bin/asmcmd afd_scan
```

8. Start the databases and mount the disk group on all nodes:

```
$ $ORACLE_HOME/bin/srvctl start diskgroup -diskgroup diskgroup
```

Migrating Oracle ASM Disk Groups with Oracle Cluster Registry or Voting Files

To migrate Oracle ASM disk groups with Oracle Cluster Registry (OCR) or voting files to Oracle ASM Filter Driver (Oracle ASMFD):

1. Log in as the root user and list the disk groups with OCR and voting files by running the following commands on one node:

```
# $ORACLE_HOME/bin/ocrcheck -config
# $ORACLE_HOME/bin/crsctl query css votedisk
```

2. As the Oracle Grid Infrastructure owner list the disks associated with the disk groups:

```
$ $ORACLE_HOME/bin/asmcmd lsdsk -G disk_group
```

3. As root, stop the databases and Oracle Clusterware on all nodes:

```
# $ORACLE_HOME/bin/crsctl stop cluster -all
```

4. As the Oracle Grid Infrastructure owner label all existing disks in the disk group by running the following command for each disk on a Hub node:

```
$ $ORACLE_HOME/bin/asmcmd afd_label label disk_path --migrate
```

5. As the Oracle Grid Infrastructure owner rescan the disks on all Hub nodes by running the following command on all of the Hub nodes:

```
$ $ORACLE_HOME/bin/asmcmd afd_scan
```

6. As root, start the Oracle Clusterware stack on all nodes and mount the OCR and voting files disk groups and databases:

```
# $ORACLE_HOME/bin/crsctl start cluster -all
```

Migrating Oracle ASM Disk Groups in an Oracle Grid Infrastructure Standalone (Oracle Restart) Environment

To migrate your existing Oracle ASM disk groups to Oracle ASM Filter Driver in an Oracle Grid Infrastructure standalone environment, perform the following steps:

1. Log in as the Oracle Grid Infrastructure standalone server owner to run the steps in this procedure.

2. List the existing disk groups:

```
$ $ORACLE_HOME/bin/asmcmd lsdg
```

3. List the existing disks:

```
$ $ORACLE_HOME/bin/asmcmd lsdsk -G diskgroup_name
```

4. Check if the status of your Oracle ASM instance is active:

```
$ $ORACLE_HOME/bin/srvctl status asm
```

5. Stop all the databases and dismount all disk groups. For each database, run the following commands:

```
$ $ORACLE_HOME/bin/srvctl stop database -db db_unique_name
```

```
$ /$ORACLE_HOME/bin/srvctl stop diskgroup -diskgroup diskgroup_name -f
```

6. Label all existing disks in the disk group by running the following command for each disk:

```
$ $ORACLE_HOME/bin/asmcmd afd_label label disk_path --migrate
```

7. Rescan the disks:

```
$ $ORACLE_HOME/bin/asmcmd afd_scan
```

8. Start the database and mount the disk group:

```
$ $ORACLE_HOME/bin/srvctl start diskgroup -diskgroup diskgroup_name
```

Determining Whether Oracle ASM Filter Driver Has Been Configured

The value of the `AFD_STATE` parameter of `SYS_ASMFD_PROPERTIES` specifies whether Oracle ASMFD is configured for the Oracle ASM instance.

You can check the state of Oracle ASMFD with the `ASMCMD afd_state` command. For example:

```
$ $ORACLE_HOME/bin/asmcmd afd_state
ASMCMD-9526: The AFD state is 'LOADED' and filtering is 'DEFAULT' on host
'myhost'
```

For information about using the `ASMCMD afd_state` command to determine the state of Oracle ASMFD, refer to “[afd_state](#)”.

To determine if Oracle ASMFD is present on the host, you can also display the value of `AFD_STATE` from `SYS_CONTEXT`. You must run the query on the Oracle ASM instance.

If the value of `AFD_STATE` is equal to `NOT AVAILABLE`, then Oracle ASMFD is not configured.

```
SQL> SELECT SYS_CONTEXT('SYS_ASMFD_PROPERTIES', 'AFD_STATE') FROM DUAL;
SYS_CONTEXT('SYS_ASMFD_PROPERTIES', 'AFD_STATE')
```

```
-----
NOT AVAILABLE
```

A value of `CONFIGURED` means that Oracle ASMFD is completely set up and the Oracle ASM instance can register with the driver.

```
SQL> SELECT SYS_CONTEXT('SYS_ASMFD_PROPERTIES', 'AFD_STATE') FROM DUAL;
SYS_CONTEXT('SYS_ASMFD_PROPERTIES', 'AFD_STATE')
```

```
-----
CONFIGURED
```

Updating the Oracle ASM Filter Driver `AFD_DISKSTRING` Parameter

The `AFD_DISKSTRING` parameter specifies the Oracle ASMFD disk discovery string that is used to identify the disks to be managed by Oracle ASMFD.

You can set and display the `AFD_DISKSTRING` parameter with the `ASMCMD afd_dsset` and `afd_dgset` commands. For example:

```
$ $ORACLE_HOME/bin/asmcmd afd_dsset '/dev/rdisk/mydisks/*'

$ $ORACLE_HOME/bin/asmcmd afd_dsget
AFD discovery string: /dev/rdisk/mydisks/*
```

For information about `ASMCMD` commands to display and set the Oracle ASMFD disk discovery string, refer to “[afd_dsget](#)” and “[afd_dsset](#)”.

You can also set the `AFD_DISKSTRING` with the `ALTER SYSTEM SQL` statement. A label is created in the disk header of those disks identified by the Oracle ASMFD disk discovery string.

```
SQL> ALTER SYSTEM AFD_DISKSTRING SET '/dev/disk0','/dev/disk1','/devices/dsk/*';
System altered.
```

You can retrieve the value of `AFD_DISKSTRING` parameter with the following query.

```
SQL> SELECT SYS_CONTEXT('SYS_ASMFD_PROPERTIES', 'AFD_DISKSTRING') FROM DUAL;
SYS_CONTEXT('SYS_ASMFD_PROPERTIES', 'AFD_DISKSTRING')
-----
'/dev/disk0','/dev/disk1','/devices/dsk/*'
```

Updating the Oracle ASM `ASM_DISKSTRING` Parameter for Oracle ASM Filter Driver Disks

You can update the Oracle ASM disk discovery string to add or remove Oracle ASMFD disk label names to and from the `ASM_DISKSTRING` initialization parameter.

For example, you can add the Oracle ASMFD disks to the `ASM_DISKSTRING` initialization parameter as follows:

```
ASM_DISKSTRING = 'AFD:DISK0', 'AFD:DISK1', '/dev/rdisk/mydisks/*'
```

Or you can set the `ASM_DISKSTRING` initialization parameter as follows:

```
ASM_DISKSTRING = 'AFD:*', '/dev/rdisk/mydisks/*'
```

You can display and set the Oracle ASM disk discovery string with the `ASMCMD dsget` and `dsset` commands. For example, you can set the Oracle ASM disk discovery string to add Oracle ASMFD disks as follows:

```
$ $ORACLE_HOME/bin/asmcmd dsset 'AFD:*', '/dev/rdisk/mydisks/*'
```

You can remove previously added Oracle ASMFD disks as follows:

```
$ $ORACLE_HOME/bin/asmcmd dsset '/dev/rdisk/mydisks/*'
```

For information about `ASMCMD` commands to display and set the Oracle ASM disk discovery string, refer to “[dsget](#)” and “[dsset](#)”.

For information about the `ASM_DISKSTRING` initialization parameter, refer to “[ASM_DISKSTRING](#)”.

Setting, Clearing, and Scanning Oracle ASM Filter Driver Labels

Setting a label provisions a disk to be used by Oracle ASMFD. After the label is set, the specified disk is managed by Oracle ASMFD.

You can add, remove, and scan labels with the `ASMCMD afd_label`, `afd_unlabel`, and `afd_scan` commands. For example:

```
$ $ORACLE_HOME/bin/asmcmd afd_label 'disk0' '/dev/rdisk/mydisks/disk0'
```

```
$ $ORACLE_HOME/bin/asmcmd afd_unlabel 'disk0'
```

```
$ $ORACLE_HOME/bin/asmcmd afd_scan '/dev/rdisk/mydisks/*'
```

For information about `ASMCMD` commands to add and remove labels on Oracle ASMFD disks, refer to “[afd_label](#)”, “[afd_unlabel](#)”, and “[afd_scan](#)”. In addition, `ASMCA` provides support for adding and removing labels on Oracle ASMFD disks. For information about using `ASMCA` to administer disk groups, refer to “[Managing Disk Groups with ASMCA](#)”.

You can also manage labels with SQL statements. You can set a label with the `ALTER SYSTEM LABEL SET SQL` statement. For example:

```
SQL> ALTER SYSTEM LABEL SET 'disk0' TO '/dev/disk0';
System altered.
```

```
SQL> SELECT UPPER(path) FROM V$ASM_DISK ORDER BY PATH;
UPPER(PATH)
```

```
AFD:DISK0
```

When you run the statement, you can use the optional `RENAME` or `MIGRATE` option. If a disk was previously provisioned for Oracle ASMFD, you can rename the label with the `RENAME` option. Note that the device should not be managed with Oracle ASMFD when the command is run. If a disk was previously used for an Oracle ASM disk group and the disk group has been dismounted, then you can label this disk using the `MIGRATE` option.

You can use `ALTER SYSTEM LABEL CLEAR` to remove the label from a device and stop Oracle ASMFD from managing the device. For example:

```
SQL> ALTER SYSTEM LABEL CLEAR 'disk0';
System altered.
```

You can use `ALTER SYSTEM LABEL SCAN` on remote nodes after the `ALTER SYSTEM LABEL SET` command is run on the local node.

Because `ALTER SYSTEM LABEL SET` statement writes the label on the disk header and the disk is shared across nodes, the same statement is not run on other nodes of the cluster.

If the device-path is not specified, then the statement uses the `AFD_DISKSTRING` parameter value to perform the scan operation.

```
SQL> ALTER SYSTEM LABEL SCAN
```

Deconfiguring Oracle ASM Filter Driver

You can deconfigure Oracle ASM Filter Driver (Oracle ASMFD) if it has been configured on your system.

This section contains the following topics:

- [“Deconfiguring Oracle ASM Filter Driver in an Oracle Grid Infrastructure Clusterware Environment”](#)
- [“Deconfiguring Oracle ASM Filter Driver in an Oracle Grid Infrastructure Standalone \(Oracle Restart\) Environment”](#)

For information about the `ASMCMD` commands for administering Oracle ASMFD, refer to [“ASMCMD Oracle ASM Filter Driver Management Commands”](#).

See Also:

Oracle Clusterware Administration and Deployment Guide for information about using `CRSCTL` commands

Deconfiguring Oracle ASM Filter Driver in an Oracle Grid Infrastructure Clusterware Environment

Perform the following steps to deconfigure Oracle ASM Filter Driver in an Oracle Clusterware environment:

1. Update the Oracle ASM disk discovery string to enable Oracle ASM to discover disk devices after Oracle ASMFD is deconfigured.

For information about updating the Oracle ASM disk discovery string, refer to [“Updating the Oracle ASM ASM_DISKSTRING Parameter for Oracle ASM Filter Driver Disks”](#).

2. As the Oracle Grid Infrastructure owner list the nodes and node roles in your cluster by running the following command on any node:

```
$ $ORACLE_HOME/bin/olsnodes -a
```

3. On each Hub node, do the following, either in rolling or non-rolling mode:

- a. Log in as the `root` user and stop Oracle Grid Infrastructure:

```
# $ORACLE_HOME/bin/crsctl stop crs
```

If the command returns any error, then stop Oracle Grid Infrastructure forcibly as follows:

```
# $ORACLE_HOME/bin/crsctl stop crs -f
```

- b. As `root`, stop Oracle ACFS kernel modules to ensure the most reliable shutdown:

```
# $ORACLE_HOME/bin/acfsload stop
```

For information about the `acfsload` command, refer to [“acfsload”](#).

- c. As `root`, deconfigure Oracle ASMFD:

```
# $ORACLE_HOME/bin/asmcmd afd_deconfigure
```

- d. As `root`, start ACFS kernel modules:

```
# $ORACLE_HOME/bin/acfsload start
```

For information about the `acfsload` command, refer to [“acfsload”](#).

- e. As `root`, start the Oracle Clusterware stack on the node:

```
# $ORACLE_HOME/bin/crsctl start crs
```

- f. As the Oracle Grid Infrastructure owner verify the status of Oracle ASMFD:

```
$ $ORACLE_HOME/bin/asmcmd afd_state
```

For information about checking on the state of the Oracle ASM Filter Driver, refer to [“Determining Whether Oracle ASM Filter Driver Has Been Configured”](#).

4. As the Oracle Grid Infrastructure owner update the Oracle ASM discovery string to remove the Oracle ASMFD path:

```
$ $ORACLE_HOME/bin/asmcmd dsget
```

```
$ $ORACLE_HOME/bin/asmcmd dsset old_diskstring
```

Check the current value of the Oracle ASM disk discovery string before updating the value. The `old_diskstring` value is the old disk discovery string value before updating with the AFD: (Oracle ASMFD) paths.

For information about updating the Oracle ASM discovery string, refer to [“Updating the Oracle ASM ASM_DISKSTRING Parameter for Oracle ASM Filter Driver Disks”](#).

For information about updating the Oracle ASM Filter Driver discovery disk discovery string, refer to [“Updating the Oracle ASM Filter Driver AFD_DISKSTRING Parameter”](#).

Deconfiguring Oracle ASM Filter Driver in an Oracle Grid Infrastructure Standalone (Oracle Restart) Environment

Perform the following steps to deconfigure Oracle ASM Filter Driver in an Oracle Grid Infrastructure standalone environment:

1. Update the Oracle ASM disk discovery string to enable Oracle ASM to discover disk devices after Oracle ASMFD is deconfigured.

For information about updating the Oracle ASM disk discovery string, refer to [“Updating the Oracle ASM ASM_DISKSTRING Parameter for Oracle ASM Filter Driver Disks”](#).

2. Log in as the `root` user and stop Oracle Grid Infrastructure for a standalone server using the following command:

```
# $ORACLE_HOME/bin/crsctl stop has
```

If the previous command returns an error, then use the following command:

```
# $ORACLE_HOME/bin/crsctl stop has -f
```

3. As `root`, stop Oracle ACFS kernel modules to ensure the most reliable shutdown:

```
# $ORACLE_HOME/bin/acfsload stop
```

For information about the `acfsload` command, refer to [“acfsload”](#).

4. As `root`, deconfigure Oracle ASMFD:

```
# $ORACLE_HOME/bin/asmcmd afd_deconfigure
```

5. As `root`, start ACFS kernel modules:

```
# $ORACLE_HOME/bin/acfsload start
```

For information about the `acfsload` command, refer to [“acfsload”](#).

6. As `root`, start Oracle Grid Infrastructure for a standalone server:

```
# $ORACLE_HOME/bin/crsctl start has
```

7. As the Oracle Grid Infrastructure standalone server owner verify the Oracle ASMFD status:

```
$ $ORACLE_HOME/bin/asmcmd afd_state
```

For information about checking on the state of the Oracle ASM Filter Driver, refer to [“Determining Whether Oracle ASM Filter Driver Has Been Configured”](#).

8. As the Oracle Grid Infrastructure standalone server owner update the Oracle ASM disk discovery string to remove the Oracle ASMFD paths:

```
$ $ORACLE_HOME/bin/asmcmd dsget
```

```
$ $ORACLE_HOME/bin/asmcmd dsset old_diskstring
```

Check the current value of the Oracle ASM disk discovery string before updating the value. The *old_diskstring* value is the old disk discovery string value before updating with the AFD: (Oracle ASMFDD) paths.

For information about updating the Oracle ASM discovery string, refer to [“Updating the Oracle ASM ASM_DISKSTRING Parameter for Oracle ASM Filter Driver Disks”](#).

For information about updating the Oracle ASM Filter Driver discovery disk discovery string, refer to [“Updating the Oracle ASM Filter Driver AFD_DISKSTRING Parameter”](#).

Authentication for Accessing Oracle ASM Instances

An Oracle ASM instance does not have a data dictionary, so the only way to connect to an Oracle ASM instance is by using one of three system privileges, SYSASM, SYSDBA, or SYSOPER. There are three modes of connecting to Oracle ASM instances:

- Local connection using operating system authentication
- Local connection using password authentication
- Remote connection by way of Oracle Net Services using password authentication

See Also:

Your operating system-specific *Oracle Grid Infrastructure Installation Guide* for information about how to ensure that the Oracle ASM and database instances have member disk access

This section describes the following topics:

- [About Privileges for Oracle ASM](#)
- [Creating Users with the SYSASM Privilege](#)
- [Operating System Authentication for Oracle ASM](#)
- [Password File Authentication for Oracle ASM](#)
- [Managing a Shared Password File in a Disk Group](#)

The Oracle ASM and database instances must have read/write operating system access rights to disk groups. For example, the Oracle ASM instance and the database instance must have identical read and write permissions for the disks that comprise the related Oracle ASM disk group. For Linux and UNIX systems, this is typically provided through shared Linux and UNIX group membership (OSASM group). On Windows systems, the Oracle ASM service must be run as Administrator. For information about file permissions and Oracle ASM File Access Control, see [“Managing Oracle ASM File Access Control for Disk Groups”](#).

See Also:

Oracle Database Security Guide for information about maintaining database security, including assigning passwords

About Privileges for Oracle ASM

During Oracle ASM installation, you can use one operating system group for all users or divide system privileges so that database administrators, storage administrators, and database operators each have distinct operating system privilege groups.

Whether you create separate operating system privilege groups or use one group to provide operating system authentication for all system privileges, you should use SYSASM to administer an Oracle ASM instance. The SYSDBA privilege cannot be used to administer an Oracle ASM instance. If you use the SYSDBA privilege to run administrative commands on an Oracle ASM instance, the operation results in an error. The SYSDBA privilege is intended to be used by the database to access disk groups.

Oracle also recommends the use of a less privileged user, such as ASMSNMP with SYSDBA privileges that is created during installation, for monitoring the Oracle ASM instance.

Operating system authentication using membership in the group or groups designated as OSDBA, OSOPER, and OSASM is valid on all Oracle platforms. Connecting to an Oracle ASM instance as SYSASM grants you full access to all of the available Oracle ASM disk groups and management functions.

This section contains these topics:

- [Using One Operating System Group for Oracle ASM Users](#)
- [Using Separate Operating System Groups for Oracle ASM Users](#)
- [The SYSASM Privilege for Administering Oracle ASM](#)
- [The SYSDBA Privilege for Managing Oracle ASM Components](#)

For information about privileges and Oracle ACFS, see [“Oracle ACFS and File Access and Administration Security”](#).

Using One Operating System Group for Oracle ASM Users

If you do not want to divide the privileges for system access into separate operating system groups, then you can designate one operating system group as the group whose members are granted access as OSDBA, OSOPER, and OSASM for Oracle ASM privileges. The default operating system group name for all of these is usually dba and that group is typically chosen for the default configuration.

[Table 1](#) shows an example of a Linux deployment without separated privileges for Oracle ASM users.

Table 1 One operating system group and one set of privileges for all Oracle ASM users

Role/Software Owner	User	Group/Privilege
Oracle ASM administrator/Oracle Grid Infrastructure home	oracle	dba/SYSASM, SYSDBA, SYSOPER
Database administrator 1/Database home 1	oracle	dba/SYSASM, SYSDBA, SYSOPER
Database administrator 2/Database home 2	oracle	dba/SYSASM, SYSDBA, SYSOPER
Operating system disk device owner	oracle	dba

Using Separate Operating System Groups for Oracle ASM Users

You can designate separate operating system groups as the operating system authentication groups for privileges on Oracle ASM. The following list describes the separate operating system authentication groups for Oracle ASM and the privileges that their members are granted.

- **OSASM group**
This group is granted the SYSASM privilege, which provides full administrative privileges for the Oracle ASM instance. For example, the group could be `asmadmin`.
- **OSDBA for Oracle ASM group**
This group is granted the SYSDBA privilege on the Oracle ASM instance, which grants access to data stored on Oracle ASM. This group has a subset of the privileges of the OSASM group.

When you implement separate administrator privileges, choose an OSDBA group for the Oracle ASM instance that is different than the group that you select for the database instance, such as `dba`. For example, the group could be `asmdba`.
- **OSOPER for Oracle ASM group**
This group is granted the SYSOPER privilege on the Oracle ASM instance, which provides operations such as startup, shutdown, mount, dismount, and check disk group. This group has a subset of the privileges of the OSASM group. For example, the group could be `asmoper`.

When you implement separate Oracle ASM and database administrator duties, this configuration requires different group and different software owners. Implicitly this implementation requires that the OSASM and OSDBA are different groups. For this configuration, you must create an OSDBA for Oracle ASM group and a database instance must be a member of that group to access the Oracle ASM instance.

In an installation that has been configured as Oracle Grid Infrastructure, the Oracle ASM user, such as `grid`, does not have to be a member of the Oracle Database OSDBA group, such as `dba1` or `dba2`, because the Oracle Clusterware database agent runs as the database owner and can use SYSDBA to connect to the database.

However, in an Oracle Restart configuration, the Oracle ASM user (`grid`) must be a member of the OSDBA group (`dba1`, `dba2`, ...) of every database. This requirement is necessary because Oracle Restart software runs as the Oracle ASM user (`grid`) and this user must be able to start and stop the databases using the `CONNECT / AS SYSDBA` authentication.

Additionally, the owner of the operating system disk devices should be the same as the owner of the Oracle ASM software.

[Table 2](#) shows an example of a Linux deployment using separate operating system privilege groups for Oracle ASM users.

Table 2 Separated operating system groups and privileges for Oracle ASM users

Role/Software Owner	User	Group/Privilege
Oracle ASM administrator/Oracle Grid Infrastructure home	<code>grid</code>	<code>asmadmin</code> (OSASM)/SYSASM <code>asmdba</code> (OSDBA for ASM)/SYSDBA <code>asmoper</code> (OSOPER for ASM)/SYSOPER

Role/Software Owner	User	Group/Privilege
Database administrator 1/Database home 1	oracle1	dba1, dba2, ... (OSDBA for the databases when in an Oracle Restart configuration) asmdba (OSDBA for ASM)/SYSDBA oper1 (OSOPER for database 1)/SYSOPER dba1 (OSDBA for database 1)/SYSDBA
Database administrator 2/Database home 2	oracle2	asmdba (OSDBA for ASM)/SYSDBA oper2 (OSOPER for database 2)/SYSOPER dba2 (OSDBA for database 2)/SYSDBA
Operating system disk device owner	grid	asmadmin (OSASM)

The SYSASM Privilege for Administering Oracle ASM

SYSASM is a system privilege that enables the separation of the SYSDBA database administration privilege from the Oracle ASM storage administration privilege. Access to the SYSASM privilege is granted by membership in an operating system group that is designated as the OSASM group. This is similar to SYSDBA and SYSOPER privileges, which are system privileges granted through membership in the groups designated as the OSDBA and OSOPER operating system groups. You can designate one group for all of these system privileges, or you can designate separate groups for each operating system privilege.

You can also grant the SYSASM privilege with password file authentication, as discussed in "[Password File Authentication for Oracle ASM](#)".

To connect locally as SYSASM using password authentication with SQL*Plus, use the following statement:

```
sqlplus SYS AS SYSASM
...
Enter password:
```

To connect remotely as SYSASM using password authentication with SQL*Plus, use the following statement:

```
sqlplus sys@"myhost.mydomain.com:1521/+ASM" AS SYSASM
...
Enter password:
```

In the previous example, +ASM is the service name of the Oracle ASM instance.

To connect locally as SYSASM to an Oracle ASM instance using operating system authentication with SQL*Plus, use the following statement:

```
sqlplus / AS SYSASM
```

The SYSDBA Privilege for Managing Oracle ASM Components

You can connect as SYSDBA to use SQL*Plus or ASMCMD commands to manage Oracle ASM components associated with the database. When running SQL or ASMCMD operations with the SYSDBA privilege, connect to the database instance rather than the Oracle ASM instance.

Connecting as SYSDBA to the database instance has a limited set of Oracle ASM privileges. For example, you cannot create a disk group when connected with the SYSDBA privilege.

When connected as SYSDBA to the database instance, the Oracle ASM operations are limited to:

- Create and delete files, aliases, directories, and templates
- Examine various Oracle ASM instance views
- Operate on files that were created by this user or only access files to which another user had explicitly granted access
- Granting Oracle ASM File Access Control to other users

Creating Users with the SYSASM Privilege

When you are logged in to an Oracle ASM instance as SYSASM, you can use the combination of CREATE USER and GRANT SQL statements to create a user who has the SYSASM privilege. You also can revoke the SYSASM privilege from a user using the REVOKE command, and you can drop a user from the password file using the DROP USER command.

Note:

- These commands update the password file for the local Oracle ASM instance only.
 - Oracle ASM does not support the creation of external and global users.
-
-

The following example describes how to perform these SQL operations for the user identified as *new_user*:

```
REM create a new user, then grant the SYSASM privilege
SQL> CREATE USER new_user IDENTIFIED by new_user_passwd;
SQL> GRANT SYSASM TO new_user;

REM connect the user to the ASM instance
SQL> CONNECT new_user AS SYSASM;
Enter password:

REM revoke the SYSASM privilege, then drop the user
SQL> REVOKE SYSASM FROM new_user;
SQL> DROP USER new_user;
```

When you revoke the last privilege of a user in an Oracle ASM password file, the user is not automatically deleted as is done in the Oracle Database password file. You must run DROP USER to delete a user with no privileges in an Oracle ASM password file.

For information about creating a user with Oracle ASM command-line utility (ASMCMD), see “[orapwusr](#)”.

See Also:

- *Oracle Database SQL Language Reference* for information about the CREATE USER and GRANT commands
 - *Oracle Database Administrator's Guide* for information about creating and maintaining a password file
-
-

Operating System Authentication for Oracle ASM

Membership in the operating system group designated as the OSASM group provides operating system authentication for the SYSASM system privilege. OSASM is provided exclusively for Oracle ASM. Initially, only the user that installs ASM is a member of the OSASM group, if you use a separate operating system group for that privilege. However, you can add other users. Members of the OSASM group are authorized to connect using the SYSASM privilege and have full access to Oracle ASM, including administrative access to all disk groups that are managed by that Oracle ASM instance.

On Linux and UNIX systems, dba is the default operating system group designated as OSASM, OSOPER, and OSDBA for Oracle ASM.

On Windows systems, ORA_ASMADMIN, ORA_ASMDBA, and ORA_ASMOPER are the operating system groups designated for OSASM, OSDBA and OSOPER respectively for Oracle ASM.

SQL*Plus commands, ASMCMD commands, and ASMCA use operating system authentication.

See Also:

- *Oracle Database Administrator's Guide* for more information about using operating system authentication
 - *Oracle Grid Infrastructure Installation Guide* for information about installation of the Oracle Grid Infrastructure
 - *Oracle Database Installation Guide* for your specific operating system for information about default operating system groups
-

Password File Authentication for Oracle ASM

Password file authentication for Oracle ASM can work both locally and remotely. To enable password file authentication, you must create a password file for Oracle ASM.

If you select the Oracle ASM storage option, then ASMCA creates a password file for Oracle ASM with initial users (SYS and ASMSNMP) when ASMCA configures the Oracle ASM disk groups. To add other users to the password file, you can use the CREATE USER and GRANT commands as described previously in the section titled "[About Privileges for Oracle ASM](#)".

If you configure an Oracle ASM instance without using ASMCA, then you must manually create a password file and grant the SYSASM privilege to user SYS.

SQL*Plus commands use password file authentication.

See Also:

- *Oracle Database Administrator's Guide* for information about creating and maintaining a password file
 - *Oracle Database SQL Language Reference* for information about the `CREATE USER` and `GRANT` commands
 - *Oracle Database Security Guide* for information about database security
 - *Oracle Database Reference* for information about the `V$PWFILERS` view which lists users who have been granted `SYSASM`, `SYSDBA`, and `SYSOPER` privileges as derived from the password file.
-
-

Managing a Shared Password File in a Disk Group

You can manage a shared password file on a disk group enabling access to the single file across the cluster system.

This sections contains these topics:

- [About a Shared Password File in a Disk Group](#)
- [Creating a Password File in a Disk Group](#)
- [Backing Up and Restoring an Oracle ASM Password File in a Disk Group](#)

For information about `ASMCMD` commands to manage an Oracle ASM or database instance password file in a disk group; such as `pwcopy`, `pwcreate`, and `pwmove`; refer to "[ASMCMD Instance Management Commands](#)".

See Also:

- *Oracle Database Administrator's Guide* for information about maintaining a password file
 - *Oracle Database Reference* for information about the `REMOTE_LOGIN_PASSWORDFILE` initialization parameter
 - *Oracle Real Application Clusters Administration and Deployment Guide* for information about `SRVCTL`
-
-

About a Shared Password File in a Disk Group

An individual password file for Oracle Database or Oracle ASM can reside on a designated Oracle ASM disk group. Having the password files reside on a single location accessible across the cluster reduces maintenance costs and situations where passwords become out of sync.

You can use a password file located on a disk group for authentication only if the Oracle ASM instance is running and the designated disk group is mounted. Otherwise, operating system authentication must be used to bootstrap the startup of the Oracle ASM instance and stack.

The `COMPATIBLE.ASM` disk group attribute must be set to at least 12.1 for the disk group where the password is to be located. The `SYSASM` privilege is required to manage the Oracle ASM password file. The `SYSDBA` privilege on Oracle ASM is required to manage the database password file.

The shared password file in a disk group is managed by `ASMCMD` commands, the `ORAPWD` tool, and `SRVCTL` commands. `ORAPWD` supports the creation of password files on an Oracle ASM disk group. All other password file manipulation is performed with `ASMCMD` or `SRVCTL` commands.

Before running commands, such as `ORAPWD`, to create a password file, ensure that the `ORACLE_SID` and `ORACLE_HOME` environmental variables have been set properly. For example, before setting the password file for Oracle ASM, set the `ORACLE_SID` and `ORACLE_HOME` environmental variables to ensure that you can connect to the local Oracle ASM instance. For information about environmental variables and connecting to an Oracle ASM instance, refer to [“Connecting To and Starting Up an Oracle ASM Instance”](#).

`SRVCTL` provides commands to manage a password file in a disk group, such as the following commands for updating and displaying the location of the password file:

```
$ srvctl modify asm -pwfile location
$ srvctl modify database -db dbname -pwfile location
$ srvctl config asm
```

Creating a Password File in a Disk Group

When using `orapwd` to create a database password file in a disk group, you must specify the disk group location and database unique name.

For example:

```
$ orapwd file='+data/ORCL/orapwdb' dbuniquename='orcl'
Enter password for SYS:
```

The `asm` switch specifies that `orapwd` create an Oracle ASM password file rather than a database password file.

For example:

```
$ orapwd file='+data/ASM/orapwasm' asm=y
Enter password for SYS:
```

You can create a new password file in a disk group using a password file from a previous release.

For example:

```
$ orapwd input_file='/oraclegrid/dbs/orapwasm' file='+data/ASM/orapwasm' asm=y
Enter password for SYS:
```

Backing Up and Restoring an Oracle ASM Password File in a Disk Group

You can make a backup of the Oracle ASM password file, and if the Oracle ASM password file is lost or the disk group becomes inaccessible, then you can restore the backup password file.

This section describes the steps to back up the Oracle ASM password file to a disk group and the steps to restore the Oracle ASM password file.

The source and target disk groups must have the disk group attribute `COMPATIBLE.ASM` set to 12.1 or higher.

1. Locate the password file using the ASMCMD `pwget` command.

For example:

```
ASMCMD [+] > pwget --asm  
+DATA/orapwasm
```

2. Back up the password file to another disk group with the `pwcopy` command.

For example:

```
ASMCMD [+] > pwcopy +DATA/orapwasm +FRA/my_pwfile_backup
```

Using `pwcopy` without the `--asm` or `--dbuniquefilename` option does not change the current location of the password file. If necessary after the copy is made, you can set the current password file location with the `pwset` command.

3. Verify which password file is in the current location after making a backup with the `pwcopy` command.

For example:

```
ASMCMD [+] > pwget --asm  
+DATA/orapwasm
```

4. Verify the backup password file was created.

For example:

```
ASMCMD [+] > ls +fra/my_pwfile_backup  
my_pwfile_backup
```

5. To restore the Oracle ASM password file, you can use `pwset` or `pwcopy`.

To restore the Oracle ASM password file from the backup and use the existing location, use the `pwset` command with the `--asm` option.

For example:

```
ASMCMD [+] > pwset --asm +FRA/my_pwfile_backup
```

To restore the Oracle ASM password file from the backup to another disk group, use the `pwcopy` command with the `--asm` option.

For example:

```
ASMCMD [+] > pwcopy --asm +FRA/my_pwfile_backup +DATA2/my_orapwasm
```

The `--asm` option with the `pwset` and `pwcopy` command sets the password location for the Oracle ASM instance.

6. Verify the location of the current password file with the `pwget` command if you have changed the location.

For example:

```
ASMCMD [+] > pwget --asm  
+DATA2/my_orapwasm
```

Migration of a Database to Use Oracle ASM

With a new installation of Oracle Database and Oracle ASM, you can initially create your database and select the Oracle ASM storage option. If you have an existing Oracle Database that stores database files in the operating system file system, then you can migrate some or all of your data files to Oracle ASM storage.

Oracle provides several methods for migrating your database to Oracle ASM. Using Oracle ASM enables you to realize the benefits of automation and simplicity in managing your database storage. To migrate to Oracle ASM, you can use the methods described in the following sections:

- [About Using Oracle Recovery Manager to Migrate Databases to Oracle ASM](#)
- [Best Practices White Papers on Migrating to Oracle ASM](#)

Note:

You must upgrade to at least Oracle Database 10g before migrating your database to Oracle ASM.

About Using Oracle Recovery Manager to Migrate Databases to Oracle ASM

You can use Oracle Recovery Manager (RMAN) to manually migrate to Oracle ASM. You can also use RMAN to migrate a single tablespace or data file to Oracle ASM.

For more information, see [Performing Oracle ASM Data Migration with RMAN](#).

Best Practices White Papers on Migrating to Oracle ASM

The Oracle Maximum Availability Architecture (MAA) website provides excellent best practices technical white papers based on different scenarios, such as:

- Minimal Downtime Migration to Oracle ASM
- Platform Migration using Transportable Tablespaces
- Platform Migration using Transportable Database

See Also:

For information about Oracle ASM best practices for migrating to Oracle ASM from environments that do not use Oracle ASM, refer to the documentation at the MAA link on Oracle Technology Network:

<http://www.oracle.com/technetwork/database/features/availability/maa-096107.html>

Administering Oracle ASM Disk Groups

This chapter describes how to administer Oracle Automatic Storage Management (Oracle ASM) disk groups. This information includes how to create, alter, drop, mount, and dismount Oracle ASM disk groups. The database instances that use Oracle ASM can continue operating while you administer disk groups.

The examples in this chapter use SQL statements. These examples assume that SQL*Plus is run from the Oracle grid home where Oracle ASM is installed and the Oracle environmental variables are set to this home. The examples also assume that the Oracle ASM instance is running. This chapter contains the following topics:

- [Managing Disk Group Attributes](#)
- [Creating Disk Groups](#)
- [Altering Disk Groups](#)
- [Oracle ASM Disk Discovery](#)
- [Managing Capacity in Disk Groups](#)
- [Oracle ASM Mirroring and Disk Group Redundancy](#)
- [Performance and Scalability Considerations for Disk Groups](#)
- [Disk Group Compatibility](#)
- [Managing Oracle ASM File Access Control for Disk Groups](#)
- [Maintaining Disk Groups](#)

For information about starting up an Oracle ASM instance, refer to “[About Starting Up an Oracle ASM Instance](#)”.

For information about administering Oracle ASM disk groups with Oracle ASM Configuration Assistant (ASMCA), refer to [Managing Oracle ASM With ASMCA](#).

For information about administering Oracle ASM disk groups with ASMCMD, refer to [Managing Oracle ASM with ASMCMD](#).

See Also:

The Oracle Cloud Storage page on the Oracle Technology Network website at <http://www.oracle.com/technetwork/database/cloud-storage/index.html> for more information about Oracle ASM

Managing Disk Group Attributes

Disk group attributes are parameters that are bound to a disk group, rather than an Oracle ASM instance. Some disk group attributes can be set when a disk group is created or altered. Other disk attributes can only be set when a disk group is created or only be set when a disk group is altered.

This section contains the following topics:

- [About Viewing and Setting Disk Group Attributes](#)
- [Summary of Disk Group Attributes](#)

In addition to the disk group attributes listed in this section, template attributes are also assigned to a disk group. For information about template attributes, see [“Managing Disk Group Templates”](#).

About Viewing and Setting Disk Group Attributes

You can display disk group attributes with the `V$ASM_ATTRIBUTE` view and the `ASMCMD lsattr` command. For an example of the use of the `V$ASM_ATTRIBUTE` view, see [Example 1](#). For information about the `lsattr` command, see [“lsattr”](#).

Disk group attributes can be set with the `ATTRIBUTE` clause of the `ALTER DISKGROUP` or `CREATE DISKGROUP` SQL statement and the `ASMCMD setattr` and `mkdg` commands. For information about the `setattr` and `mkdg` commands, see [“setattr”](#) and [“mkdg”](#).

You can also set disk group attributes with Oracle ASM Configuration Assistant (ASMCA). For information about managing disk groups with ASMCA, refer to [“Managing Disk Groups with ASMCA”](#).

Summary of Disk Group Attributes

The Oracle ASM disk group attributes are listed in this section.

- `ACCESS_CONTROL.ENABLED`
- `ACCESS_CONTROL.UMASK`
- `AU_SIZE`
- `CELL.SMART_SCAN_CAPABLE`
- `CELL.SPARSE_DG`
- `COMPATIBLE.ASM`
- `COMPATIBLE.RDBMS`
- `COMPATIBLE.ADVM`
- `CONTENT.CHECK`
- `CONTENT.TYPE`
- `DISK_REPAIR_TIME`
- `FAILGROUP_REPAIR_TIME`

- [IDP.BOUNDARY](#) and [IDP.TYPE](#)
- [PHYS_META_REPLICATED](#)
- [SECTOR_SIZE](#)
- [STORAGE.TYPE](#)
- [THIN_PROVISIONED](#)

ACCESS_CONTROL.ENABLED

This attribute configures Oracle ASM File Access Control and can only be set when altering a disk group.

For information about the `ACCESS_CONTROL.ENABLED` attribute, see “[Setting Disk Group Attributes for Oracle ASM File Access Control](#)”.

ACCESS_CONTROL.UMASK

This attribute configures Oracle ASM File Access Control and can only be set when altering a disk group.

For information about the `ACCESS_CONTROL.UMASK` attribute, see “[Setting Disk Group Attributes for Oracle ASM File Access Control](#)”.

AU_SIZE

This attribute specifies allocation unit (AU) size and can only be set when creating a disk group. [Example 1](#) shows how the `AU_SIZE` is specified with the `CREATE DISKGROUP` SQL statement.

For information about allocation units, refer to “[About Oracle ASM Allocation Units](#)”.

CELL.SMART_SCAN_CAPABLE

This attribute is only applicable to the configuration of Oracle Exadata storage.

See Also:

Oracle Exadata documentation

CELL.SPARSE_DG

This attribute is only applicable to the configuration of Oracle Exadata storage.

See Also:

Oracle Exadata documentation

COMPATIBLE.ASM

This attribute specifies the Oracle ASM compatibility level of a disk group. Compatibility attributes can be set when the disk group is created and advanced when a disk group is altered, but compatibility attributes cannot be reversed. For information about the `COMPATIBLE.ASM` attribute, see “[COMPATIBLE.ASM](#)”.

COMPATIBLE.RDBMS

This attribute specifies the database compatibility level of a disk group. Compatibility attributes can be set when the disk group is created and advanced when a disk group is altered, but compatibility attributes cannot be reversed. For information about the `COMPATIBLE.RDBMS` attribute, see [“COMPATIBLE.RDBMS”](#).

COMPATIBLE.ADVM

This attribute specifies the Oracle Automatic Storage Management Cluster File System (Oracle ACFS) and Oracle ASM Dynamic Volume Manager (Oracle ADVM) compatibility level of a disk group. Compatibility attributes can be set when the disk group is created and advanced when a disk group is altered, but compatibility attributes cannot be reversed. For information about the `COMPATIBLE.ADVM` attribute, see [“COMPATIBLE.ADVM”](#) and [“Overview of Oracle ASM Dynamic Volume Manager”](#).

CONTENT.CHECK

This attribute enables or disables content checking when performing data copy operations for rebalancing a disk group. The attribute value can be set to `true` or `false`.

The content checking can include Hardware Assisted Resilient Data (HARD) checks on user data, validation of file types from the file directory against the block contents and file directory information, and mirror side comparison.

When the attribute is set to `true`, logical content checking is enabled for all rebalance operations.

For information about disk group rebalancing, refer to [“Manually Rebalancing Disk Groups”](#) and [“Tuning Rebalance Operations”](#).

CONTENT.TYPE

This attribute identifies the disk group type: `data`, `recovery`, or `system`. The type value determines where Oracle ASM places the nearest neighbor disk in the failure group where Oracle ASM mirrors copies of the data. Oracle ASM uses this attribute value to make it less likely that a double failure in the storage medium causes disk groups of different content types to become unavailable. Specifying this attribute enables Oracle ASM to better deploy all disk groups in the available storage.

The default value is `data` which specifies a distance of 1 to the nearest neighbor disk. A value of `recovery` specifies a distance of 3 to the nearest neighbor disk and a value of `system` specifies a distance of 5.

The attribute can be specified when creating or altering a disk group. If `CONTENT.TYPE` attribute is set or changed using `ALTER DISKGROUP`, then the new configuration does not take effect until a disk group rebalance is explicitly run.

The `CONTENT.TYPE` attribute is only valid for disk groups that are set to normal or high redundancy. The `COMPATIBLE.ASM` attribute must be set to `11.2.0.3` or higher to enable the `CONTENT.TYPE` attribute for the disk group.

This attribute can be set with `ASMCMD mkdg` or `SQL CREATE` and `ALTER DISKGROUP` statements.

For example:

```
SQL> CREATE DISKGROUP data NORMAL REDUNDANCY
      FAILGROUP controller1 DISK
```

```

        '/devices/disk1' NAME disk1,
    ...
    ATTRIBUTE
        'compatible.asm' = '12.1.0.1',
        'content.type' = 'recovery',
    ...
SQL> ALTER DISKGROUP data SET ATTRIBUTE 'content.type' = 'data';

```

This attribute is primarily intended for use with Oracle Exadata storage.

For information about disk resync, see “[Oracle ASM Fast Mirror Resync](#)”.

See Also:

- *Oracle Exadata documentation*
 - [My Oracle Support \(https://support.oracle.com\)](https://support.oracle.com) for information about using the CONTENT . TYPE attribute with Oracle Exadata storage
-
-

DISK_REPAIR_TIME

This attribute specifies the time interval to repair a disk and bring it back online before initiating the drop operation. This attribute can only be set when altering a disk group and is only applicable to normal and high redundancy disk groups.

For information about disk repair time, see “[Oracle ASM Fast Mirror Resync](#)”.

FAILGROUP_REPAIR_TIME

This attribute specifies a default repair time for the failure groups in the disk group. The failure group repair time is used if Oracle ASM determines that an entire failure group has failed. The default value is 24 hours (24h). If there is a repair time specified for a disk, such as with the DROP AFTER clause of the SQL ALTER DISKGROUP OFFLINE DISK statement, that disk repair time overrides the failure group repair time.

This attribute can only be set when altering a disk group and is only applicable to normal and high redundancy disk groups.

For information about failure group repair time, see “[Oracle ASM Fast Mirror Resync](#)”.

IDP.BOUNDARY and IDP.TYPE

These attributes are used to configure Oracle Exadata storage.

See Also:

Oracle Exadata documentation

PHYS_META_REPLICATED

This disk group attribute tracks the replication status of a disk group. When the Oracle ASM compatibility of a disk group is advanced to 12.1 or higher, the physical metadata of each disk is replicated. This metadata includes the disk header, free space table blocks, and allocation table blocks. The replication is performed online

asynchronously. This attribute value is set to `true` by Oracle ASM if the physical metadata of every disk in the disk group has been replicated.

This disk group attribute is only defined in a disk group with the Oracle ASM disk group compatibility (`COMPATIBLE.ASM`) set to 12.1 and higher. This attribute is read-only and is intended for information only. A user cannot set or change its value. The values are either `true` or `false`.

SECTOR_SIZE

This attribute specifies the sector size for disks in a disk group and can only be set when creating a disk group.

For information about the `SECTOR_SIZE` attribute, see [“Specifying the Sector Size for Drives”](#).

STORAGE.TYPE

This disk group attribute specifies the type of the disks in the disk group. The possible values are `AXIOM`, `ZFSSA`, and `OTHER`. If the attribute is set to `AXIOM` or `ZFSSA`, then all disks in the disk group must be of that type. If the attribute is set to `OTHER`, then any types of disks can be in the disk group.

If the `STORAGE.TYPE` disk group attribute is set to `AXIOM` or `ZFSSA`, then functionality for Hybrid Columnar Compression (HCC) can be enabled for Pillar Axiom or ZFS storage.

Note:

Pillar Axiom storage must be added as SCSI/Fiber Channel.

To set the `STORAGE.TYPE` attribute, the `COMPATIBLE.ASM` and `COMPATIBLE.RDBMS` disk group attributes must be set to 11.2.0.3 or higher. For maximum support with ZFS storage, set the `COMPATIBLE.ASM` and `COMPATIBLE.RDBMS` disk group attributes to 11.2.0.4 or higher. For information about disk group compatibility attributes, refer to [“Disk Group Compatibility”](#).

The `STORAGE.TYPE` attribute can be set when creating a disk group or when altering a disk group. The attribute cannot be set when clients are connected to the disk group. For example, the attribute cannot be set when an Oracle ADVM volume is enabled on the disk group.

The attribute is not visible in the `V$ASM_ATTRIBUTE` view or with the `ASMCMD lsattr` command until the attribute has been set.

See Also:

Oracle Database Concepts for more information about Hybrid Columnar Compression. Hybrid Columnar Compression is a feature of certain Oracle storage systems.

THIN_PROVISIONED

This attribute enables or disables the functionality to discard unused storage space after a disk group rebalance is completed. The attribute value can be `true` or `false`. The default value is `false`.

Storage vendor products that support thin provisioning have the capability to reuse the discarded storage space for a more efficient overall physical storage utilization.

Note:

The `THIN_PROVISIONED` attribute is supported only in Oracle Database 12c Release 1 with Oracle ASM Filter Driver (Oracle ASMD).

For information about disk group rebalancing, refer to [“Tuning Rebalance Operations”](#).

Creating Disk Groups

This section contains information about creating disk groups. You can use the `CREATE DISKGROUP` SQL statement to create a disk group.

This section contains the following topics:

- [Using the CREATE DISKGROUP SQL Statement](#)
- [Creating Disk Groups for Data and Fast Recovery Area](#)
- [Creating Disk Groups for a New Oracle Installation](#)
- [Specifying the Sector Size for Drives](#)
- [Storing Oracle Cluster Registry and Voting Files in Oracle ASM Disk Groups](#)

Using the CREATE DISKGROUP SQL Statement

You can use `CREATE DISKGROUP` SQL statement to create disk groups. When creating a disk group, you:

- Assign a unique name to the disk group.

The specified disk group name is not case sensitive and is always converted to uppercase when stored internally.

Note:

Oracle does not recommend using identifiers for database object names that must be quoted. While these quoted identifiers may be valid as names in the SQL `CREATE` statement, such as `CREATE DISKGROUP "1DATA"`, the names may not be valid when using other tools that manage the database object. For more information about naming database objects, refer to *Oracle Database SQL Language Reference*.

- Specify the redundancy level of the disk group.

For Oracle ASM to mirror files, specify the redundancy level as `NORMAL REDUNDANCY` (2-way mirroring by default for most file types) or `HIGH REDUNDANCY` (3-way mirroring for all files). Specify `EXTERNAL REDUNDANCY` if you do not want mirroring by Oracle ASM. For example, you might choose `EXTERNAL REDUNDANCY` to use storage array protection features.

After a disk group is created, you cannot alter the redundancy level of the disk group. To change the redundancy level, you must create another disk group with the appropriate redundancy and then move the files to the new disk group.

Oracle recommends that you create failure groups of equal size to maintain space balance and even distribution of mirror data.

For more information about redundancy levels, refer to [“Mirroring_ Redundancy_ and Failure Group Options”](#).

- Specify the disks that are to be formatted as Oracle ASM disks belonging to the disk group.

The disks can be specified using operating system dependent wildcard characters in search strings that Oracle ASM then uses to find the disks. You can specify names for the disks with the `NAME` clause or use the system-generated names.

- Optionally specify the disks as belonging to specific failure groups.

For information about failure groups, refer to [“Understanding Oracle ASM Concepts”](#) and [“Mirroring_ Redundancy_ and Failure Group Options”](#).

- Optionally specify the type of failure group.

For information about `QUORUM` and `REGULAR` failure groups, refer to [“Storing Oracle Cluster Registry and Voting Files in Oracle ASM Disk Groups”](#).

- Optionally specify disk group attributes, such as software compatibility or allocation unit size.

Oracle ASM programmatically determines the size of each disk. If for some reason this is not possible, or to restrict the amount of space used on a disk, you can specify a `SIZE` clause for each disk. Oracle ASM creates operating system-independent names for the disks in a disk group that you can use to reference the disks in other SQL statements. Optionally, you can provide your own name for a disk using the `NAME` clause. Disk names are available in the `V$ASM_DISK` view.

Note:

A disk cannot belong to multiple disk groups.

The Oracle ASM instance ensures that any disk in a newly created disk group is addressable and is not currently a member of another disk group. You must use `FORCE` only when adding a disk that was dropped with `FORCE`. If a disk is dropped with `NOFORCE`, then you can add it with `NOFORCE`. For example, a disk might have failed and was dropped from its disk group. After the disk is repaired, it is no longer part of any disk group, but Oracle ASM still recognizes that the disk had been a member of a disk group. You must use the `FORCE` flag to include the disk in a new disk group. In addition, the disk must be addressable, and the original disk group must not be mounted. Otherwise, the operation fails.

Note:

Use caution when using the `FORCE` option to add a previously used disk to a disk group; you might cause another disk group to become unusable.

The `CREATE DISKGROUP` statement mounts the disk group for the first time, and adds the disk group name to the `ASM_DISKGROUPS` initialization parameter if a server parameter file is being used. If a text initialization parameter file is being used and you want the disk group to be automatically mounted at instance startup, then you must remember to add the disk group name to the `ASM_DISKGROUPS` initialization parameter before you shut down and restart the Oracle ASM instance. You can also create disk groups with Oracle ASM Configuration Assistant (ASMCA). Refer to [“Managing Disk Groups with ASMCA”](#).

See Also:

The `CREATE DISKGROUP` SQL statement in the *Oracle Database SQL Language Reference*

Creating Disk Groups for Data and Fast Recovery Area

This topic discusses how to create a disk group for data and a disk group for the fast recovery area.

The SQL statement in [Example 1](#) creates a disk group named `data` with normal redundancy consisting of two failure groups `controller1` or `controller2` with four disks in each failure group. The `data` disk group is typically used to store database data files.

The example assumes that the `ASM_DISKSTRING` initialization parameter is set to the `'/devices/*'` string. Oracle ASM disk discovery identifies `diska1` through `diska4` and `diskb1` through `diskb4` in the `/devices` directory.

In [Example 1](#), the `NAME` clauses enable you to explicitly assign names to the disks rather than the default system-generated names. The system-generated names are in the form `diskgroup_nnnn`, where `nnnn` is the disk number for the disk in the disk group. For information about the disk name format when using Oracle ASM Filter Driver, refer to [“Oracle ASM Filter Driver”](#).

When creating the disk group in [Example 1](#), the values of following disk group attributes were explicitly set:

- `AU_SIZE`
Specifies the size of the allocation unit for the disk group. For information about allocation units, see [“About Oracle ASM Allocation Units”](#).

You can view the value of the `AU_SIZE` disk group attribute in the `ALLOCATION_UNIT_SIZE` column of the `V$ASM_DISKGROUP` view.
- `COMPATIBLE.ASM`
Determines the minimum software version for any Oracle ASM instance that uses a disk group. For information about the `COMPATIBLE.ASM` attribute, see [“COMPATIBLE.ASM”](#).
- `COMPATIBLE.RDBMS`
Determines the minimum software version for any database instance that uses a disk group. For information about the `COMPATIBLE.RDBMS` attribute, see [“COMPATIBLE.RDBMS”](#).
- `COMPATIBLE.ADVM`

Determines whether the disk group can contain Oracle ADVM volumes. For information about the `COMPATIBLE.ADVM` attribute, see [“COMPATIBLE.ADVM”](#).

In [Example 2](#), the `fra` disk group (typically created for the fast recovery area) is created with the default disk group attribute values. Names are not specified for the Oracle ASM disks and failure groups are not explicitly specified. This example assumes that `diskc1` through `diskc9` are present in the `/devices` directory.

Example 1 Creating the DATA disk group

```
CREATE DISKGROUP data NORMAL REDUNDANCY
  FAILGROUP controller1 DISK
    '/devices/diska1' NAME diska1,
    '/devices/diska2' NAME diska2,
    '/devices/diska3' NAME diska3,
    '/devices/diska4' NAME diska4
  FAILGROUP controller2 DISK
    '/devices/diskb1' NAME diskb1,
    '/devices/diskb2' NAME diskb2,
    '/devices/diskb3' NAME diskb3,
    '/devices/diskb4' NAME diskb4
  ATTRIBUTE 'au_size' = '4M',
    'compatible.asm' = '11.2',
    'compatible.rdbms' = '11.2',
    'compatible.advm' = '11.2';
```

Example 2 Creating the FRA disk group

```
CREATE DISKGROUP fra NORMAL REDUNDANCY
  DISK '/devices/diskc*';
```

Creating Disk Groups for a New Oracle Installation

This section describes the basic procedure to follow when creating disk groups during a new installation of Oracle Restart and Oracle Database. This information also applies to an Oracle Grid Infrastructure installation.

The procedure assumes that the `data` disk group is used for the storage of the database data files and the `fra` disk group is used for storage of the fast recovery area files. Detailed information about installation with Oracle Universal Installer (OUI) and database creation with Database Configuration Assistant (DBCA) is available in the installation guides for your specific operating system.

1. Install Oracle Restart with OUI, following the screen prompts.

During the installation, create the `data` disk group for storing database files such as the data and control files.

This OUI process is similar to creating a disk group with Oracle ASM Configuration Assistant (ASMCA). For information about using ASMCA to create disk groups, see [“Managing Disk Groups with ASMCA”](#).

The `data` disk group is the disk group used for storing Oracle Cluster Registry (OCR) and voting files in an Oracle Grid Infrastructure installation. See [“Storing Oracle Cluster Registry and Voting Files in Oracle ASM Disk Groups”](#)

2. After Oracle Restart is installed, use ASMCA to create the `fra` disk group for storing the fast recovery area files.

Create the `fra` disk group to hold the fast recovery area files.

At this time, you can also update the `data` disk group if necessary. For information about using ASMCA to create or alter disk groups, see [“Managing Disk Groups with ASMCA”](#).

You can also create the `fra` disk group with SQL*Plus or ASMCMD commands run from the Oracle Restart home. For information, see [“Using the CREATE DISKGROUP SQL Statement”](#) and [“mkdg”](#).

See Also:

- *Oracle Database Backup and Recovery User's Guide* for information about configuring the fast recovery area
 - *Oracle Database Administrator's Guide* for information about specifying a fast recovery area
-
-

3. Install the Oracle Database software with OUI, following the screen prompts.
4. After the database software has been installed, run DBCA to create a database, following the screen prompts.

During the creation of the database, make the appropriate selections to use Oracle ASM for storage of data files and fast recovery area files. When prompted:

- Store database data files in the `data` disk group
 - Store fast recovery area files in the `fra` disk group
-
-

See Also:

- *Oracle Grid Infrastructure Installation Guide* for your operating system for detailed information about installation of Oracle Grid Infrastructure and Oracle Restart
 - *Oracle Database Installation Guide* for your operating system for detailed information about installation of an Oracle Database
-
-

Specifying the Sector Size for Drives

You can use the optional `SECTOR_SIZE` disk group attribute with the `CREATE DISKGROUP` SQL statement to specify disks with the sector size set to the value of `SECTOR_SIZE` for the disk group. Oracle ASM provides support for 4 KB sector disk drives without negatively affecting performance. The `SECTOR_SIZE` disk group attribute can be set only during disk group creation.

The values for `SECTOR_SIZE` can be set to 512, 4096, or 4K if the disks support those values. The default value is platform dependent. The `COMPATIBLE.ASM` and `COMPATIBLE.RDBMS` disk group attributes must be set to 11.2 or higher to set the sector size to a value other than the default value.

Note:

Oracle Automatic Storage Management Cluster File System (Oracle ACFS) does not support 4 KB sector drives. There is a performance penalty for Oracle ACFS when using 4 KB sector disk drives in 512 sector emulation mode.

The following validations apply to the sector size disk group attribute.

- Oracle ASM prevents disks of different sector sizes from being added to the same disk group. This validation occurs during `CREATE DISKGROUP`, `ALTER DISKGROUP ADD DISK`, and `ALTER DISKGROUP MOUNT` operations.
- If the `SECTOR_SIZE` attribute is explicitly specified when creating a disk group, then Oracle ASM attempts to verify that all disks discovered through disk search strings have a sector size equal to the specified value. If one or more disks were found to have a sector size different from the specified value, or if Oracle ASM was not able to verify a disk sector size, then the create operation fails.

Oracle ASM also attempts to verify disk sector size during the mount operation and the operation fails if one or more disks have a sector size different than the value of the `SECTOR_SIZE` attribute.

- If the `SECTOR_SIZE` attribute is not specified when creating a disk group and Oracle ASM can verify that all discovered disks have the same sector value, then that value is assumed for the disk group sector size that is created. If the disks have different sector sizes, the create operation fails.
- When new disks are added to an existing disk group using the `ALTER DISKGROUP .. ADD DISK SQL` statement, you must ensure that the new disks to be added have the same value as the `SECTOR_SIZE` disk group attribute. If the new disks have different sector sizes, the alter operation fails.
- You can determine the sector size value that has either been assumed or explicitly set for a successful disk group creation by querying the `V$ASM_ATTRIBUTE` view or run the `ASMCMD lsattr` command. You can also query the `SECTOR_SIZE` column in the `V$ASM_DISKGROUP` view.

```
SQL> SELECT name, value FROM V$ASM_ATTRIBUTE
        WHERE name = 'sector_size' AND group_number = 1;
NAME                                VALUE
-----                                -
sector_size                          512
```

```
SQL> SELECT group_number, sector_size FROM V$ASM_DISKGROUP
        WHERE group_number = 1;
```

```
GROUP_NUMBER SECTOR_SIZE
-----
1            512
```

- Not all disks support all of the possible `SECTOR_SIZE` values. The sector size attribute setting must be compatible with the physical hardware.

As shown in [Example 3](#), you can use the `SECTOR_SIZE` attribute with the `CREATE DISKGROUP SQL` statement to specify the sector size of the disk drive on which the Oracle ASM disk group is located.

See Also:

- *Oracle Database SQL Language Reference* for information about the disk group attributes and the `CREATE DISKGROUP` SQL statement
- *Oracle Database SQL Language Reference* for information about the `BLOCKSIZE` keyword
- *Oracle Database Reference* for details about the `V$ASM_ATTRIBUTE` and `V$ASM_DISKGROUP` views

Example 3 Creating a disk group of 4K sector size

```
CREATE DISKGROUP data NORMAL REDUNDANCY
FAILGROUP controller1 DISK
'/devices/diska1',
'/devices/diska2',
'/devices/diska3',
'/devices/diska4'
FAILGROUP controller2 DISK
'/devices/diskb1',
'/devices/diskb2',
'/devices/diskb3',
'/devices/diskb4'
ATTRIBUTE 'compatible.asm' = '11.2', 'compatible.rdbms' = '11.2',
'sector_size'='4096';
```

Storing Oracle Cluster Registry and Voting Files in Oracle ASM Disk Groups

You can store Oracle Cluster Registry (OCR) and voting files in Oracle ASM disk groups. You can also store a backup of the OCR file in a disk group. Voting files and OCR are two important components of Oracle Clusterware. Voting files manage information about node membership. OCR manages cluster and Oracle Real Application Clusters (Oracle RAC) database configuration information.

A quorum failure group is a special type of failure group that does not contain user data. Quorum failure groups are used for storing Oracle ASM metadata. A quorum failure group may also contain voting files if those files are stored in a disk group that contains a quorum failure group. Additionally, Oracle ASM uses a quorum failure group to help determine if the disk group can be mounted in the event of the loss of one or more failure groups.

Because disks in quorum failure groups do not contain user data, a quorum failure group is not considered when determining redundancy requirements in respect to storing user data. For information about failure groups, see [“Oracle ASM Failure Groups”](#).

You can manage and monitor OCR and voting files with `CRSCTL` and `ocrconfig` command-line tools, `CREATE` and `ALTER DISKGROUP` SQL statements, and `V$ASM` views.

The `CRSCTL` and `ocrconfig` commands enable the placement of OCR storage and Cluster Synchronization Services (CSS) voting files inside the disk groups managed by Oracle ASM.

The `QUORUM` and `REGULAR` keywords in `CREATE` and `ALTER DISKGROUP` SQL statements enable the specification of an additional qualifier for failure groups or disks when creating or altering a disk group. Note that `QUORUM` disks (or disks in `QUORUM`

failure groups) cannot contain user data, while REGULAR disks (or disks in non-quorum failure groups) do not have this restriction.

You can use these keywords before the keyword FAILGROUP if a failure group is being explicitly specified. If the failure group is implicitly implied, you can use these keywords (QUORUM/REGULAR) before the keyword DISK. When failure groups are explicitly specified, it is an error to specify these keywords (QUORUM/REGULAR) immediately before the keyword DISK. REGULAR is the default failure group type.

When performing operations on existing disks or failure groups, the qualifier specified in the SQL must match the qualifier that was specified when the disks or failure groups were added to the disk group.

[Example 4](#) shows the creation of a disk group with a QUORUM failure group. For Oracle Clusterware files a minimum of three disk devices or three failure groups is required with a normal redundancy disk group. A QUORUM failure group is not considered when determining redundancy requirements in respect to storing user data. The COMPATIBLE.ASM disk group compatibility attribute must be set to 11.2 or greater to store OCR or voting files in a disk group.

The FAILGROUP_TYPE column in the V\$ASM_DISK or V\$ASM_DISK_STAT views specifies the failure group type. The value for this column is REGULAR for regular failure groups and QUORUM for quorum failure groups.

The VOTING_FILE column in the V\$ASM_DISK or V\$ASM_DISK_STAT views specifies whether a disk contains a voting file. The value for this column is either Y if the disk contains a voting file or N if not.

The value of USABLE_FILE_MB in V\$ASM_DISKGROUP or V\$ASM_DISKGROUP_STAT does not consider any free space that is present in QUORUM disks because that space is not available for client data files.

For information about V\$ASM views, refer to [“Views Containing Oracle ASM Disk Group Information”](#).

See Also:

- *Oracle Grid Infrastructure Installation Guide* for information about configuring voting files and Oracle Cluster Registry (OCR)
 - *Oracle Clusterware Administration and Deployment Guide* for information about managing Oracle Cluster Registry and voting files
 - *Oracle Database SQL Language Reference* for information about the CREATE DISKGROUP and ALTER DISKGROUP SQL statements
 - *Oracle Database Reference* for details about the V\$ASM* dynamic performance views
-
-

Example 4 Using the QUORUM keyword when creating a failure group

```
CREATE DISKGROUP ocr_data NORMAL REDUNDANCY
  FAILGROUP fg1 DISK '/devices/diskg1'
  FAILGROUP fg2 DISK '/devices/diskg2'
  QUORUM FAILGROUP fg3 DISK '/devices/diskg3'
  ATTRIBUTE 'compatible.asm' = '12.1.0.0.0';
```

Altering Disk Groups

You can use the `ALTER DISKGROUP` SQL statement to alter a disk group configuration. You can add, resize, or drop disks while the database remains online. Whenever possible, multiple operations in a single `ALTER DISKGROUP` statement are recommended. Grouping operations in a single `ALTER DISKGROUP` statement can reduce rebalancing operations.

Oracle ASM automatically rebalances when the configuration of a disk group changes. By default, the `ALTER DISKGROUP` statement does not wait until the operation is complete before returning. Query the `V$ASM_OPERATION` view to monitor the status of this operation.

Use the `REBALANCE WAIT` clause to cause the `ALTER DISKGROUP` statement processing to wait until the rebalance operation is complete before returning. This is especially useful in scripts. The statement also accepts a `REBALANCE NOWAIT` clause that invokes the default behavior of conducting the rebalance operation asynchronously in the background.

You can interrupt a rebalance running in wait mode by typing `CTRL+C` on most platforms. This causes the statement to return immediately with the message `ORA-01013: user requested cancel of current operation`, and then to continue the operation asynchronously. Typing `CTRL+C` does not cancel the rebalance operation or any disk add, drop, or resize operations.

To control the speed and resource consumption of the rebalance operation, you can include the `REBALANCE POWER` clause in statements that add, drop, or resize disks. Refer to “[Manually Rebalancing Disk Groups](#)” for more information about this clause.

This section contains the following topics:

- [Managing Oracle ADVM Volumes in a Disk Group](#)
- [Adding Disks to a Disk Group](#)
- [Using the ALTER DISKGROUP SQL Statement to Add Disks to a Disk Group](#)
- [Replacing Disks in Disk Groups](#)
- [Renaming Disks in Disk Groups](#)
- [Dropping Disks from Disk Groups](#)
- [Intelligent Data Placement](#)
- [Resizing Disks in Disk Groups](#)
- [Undropping Disks in Disk Groups](#)
- [Manually Rebalancing Disk Groups](#)
- [Tuning Rebalance Operations](#)
- [Scrubbing Disk Groups](#)

See Also:

The `ALTER DISKGROUP` SQL statement in the *Oracle Database SQL Language Reference*

Managing Oracle ADVM Volumes in a Disk Group

You can create an Oracle ASM Dynamic Volume Manager (Oracle ADVM) volume in a disk group. The volume device associated with the dynamic volume can then be used to host an Oracle ACFS file system.

The compatibility parameters `COMPATIBLE.ASM` and `COMPATIBLE.ADVM` must be set to 11.2 or higher for the disk group. See [“Disk Group Compatibility Attributes”](#).

The `ALTER DISKGROUP VOLUME` SQL statements enable you to manage Oracle ADVM volumes, including the functionality to add, modify, resize, disable, enable, and drop volumes. The following are examples of the `ALTER DISKGROUP VOLUME` statement.

If the volume is hosting an Oracle ACFS file system, then you cannot resize that volume with the SQL `ALTER DISKGROUP` statement. Instead you must use the `acfsutil size` command. For information, see [“acfsutil size”](#).

For information about Oracle ADVM, see [“Overview of Oracle ASM Dynamic Volume Manager”](#). For information about managing Oracle ADVM volumes with `ASMCMD`, see [Managing Oracle ADVM with ASMCMD](#). For information about managing Oracle ADVM volumes with `ASMCA`, see [“ASMCA GUI Tool for Managing Oracle ACFS and Oracle ADVM”](#).

See Also:

The `ALTER DISKGROUP` SQL statement in the *Oracle Database SQL Language Reference*

Example 5 Managing volumes with ALTER DISKGROUP VOLUME statements

```
SQL> ALTER DISKGROUP data ADD VOLUME volume1 SIZE 10G;
Diskgroup altered.
```

```
SQL> ALTER DISKGROUP data RESIZE VOLUME volume1 SIZE 15G;
Diskgroup altered.
```

```
SQL> ALTER DISKGROUP data DISABLE VOLUME volume1;
Diskgroup altered.
```

```
SQL> ALTER DISKGROUP data ENABLE VOLUME volume1;
Diskgroup altered.
```

```
SQL> ALTER DISKGROUP ALL DISABLE VOLUME ALL;
Diskgroup altered.
```

```
SQL> ALTER DISKGROUP data DROP VOLUME volume1;
Diskgroup altered.
```

Adding Disks to a Disk Group

You can use the `ADD` clause of the `ALTER DISKGROUP` statement to add a disk or a failure group to a disk group. You can use the same syntax with the `ALTER DISKGROUP` statement that you use to add a disk or failure group with the `CREATE DISKGROUP` statement. For an example of the `CREATE DISKGROUP` SQL statement,

refer to [Example 1](#) . After you add new disks, the new disks gradually begin to accommodate their share of the workload as rebalancing progresses.

Using SQL statements to add disks to a disk group is illustrated in [“Using the ALTER DISKGROUP SQL Statement to Add Disks to a Disk Group”](#) . You can also add disks to a disk group with ASMCA. Refer to [“Managing Disk Groups with ASMCA”](#) .

Using the ALTER DISKGROUP SQL Statement to Add Disks to a Disk Group

The SQL statements presented in the following example demonstrate the interactions of disk discovery with the ADD DISK operation.

Assume that disk discovery identifies the following disks in directory /devices:

```
/devices/diska1 -- member of data1
/devices/diska2 -- member of data1
/devices/diska3 -- member of data1
/devices/diska4 -- member of data1
/devices/diska5 -- candidate disk
/devices/diska6 -- candidate disk
/devices/diska7 -- candidate disk
/devices/diska8 -- candidate disk

/devices/diskb1 -- member of data1
/devices/diskb2 -- member of data1
/devices/diskb3 -- member of data1
/devices/diskb4 -- member of data2

/devices/diskc1 -- member of data2
/devices/diskc2 -- member of data2
/devices/diskc3 -- member of data3
/devices/diskc4 -- candidate disk

/devices/diskd1 -- candidate disk
/devices/diskd2 -- candidate disk
/devices/diskd3 -- candidate disk
/devices/diskd4 -- candidate disk
/devices/diskd5 -- candidate disk
/devices/diskd6 -- candidate disk
/devices/diskd7 -- candidate disk
/devices/diskd8 -- candidate disk
```

You can query the V\$ASM_DISK view to display the status of Oracle ASM disks. See [“Views Containing Oracle ASM Disk Group Information”](#) .

The following statement would fail because /devices/diska1 through /devices/diska4 currently belong to the disk group data1.

```
ALTER DISKGROUP data1 ADD DISK
    '/devices/diska*';
```

The following statement successfully adds disks /devices/diska5 through /devices/diska8 to data1. Because no FAILGROUP clauses are included in the ALTER DISKGROUP statement, each disk is assigned to its own failure group. The NAME clauses assign names to the disks, otherwise they would have been assigned system-generated names.

```
ALTER DISKGROUP data1 ADD DISK
    '/devices/diska5' NAME diska5,
    '/devices/diska6' NAME diska6,
    '/devices/diska7' NAME diska7,
    '/devices/diska8' NAME diska8;
```


The following statement would fail because the search string matches disks that are contained in other disk groups. Specifically, `/devices/diska4` belongs to disk group `data1` and `/devices/diskb4` belongs to disk group `data2`.

```
ALTER DISKGROUP data1 ADD DISK
    '/devices/disk*4';
```

The following statement would successfully add `/devices/diskd1` through `/devices/diskd8` to disk group `data1`. This statement runs with a rebalance power of 5, and does not return until the rebalance operation is complete.

```
ALTER DISKGROUP data1 ADD DISK
    '/devices/diskd*'
    REBALANCE POWER 5 WAIT;
```

If `/devices/diskc3` was previously a member of a disk group that no longer exists, then you could use the `FORCE` option to add the disk as a member of another disk group. For example, the following use of the `FORCE` clause enables `/devices/diskc3` to be added to `data2`, even though it is a current member of `data3`. For this statement to succeed, `data3` cannot be mounted.

```
ALTER DISKGROUP data2 ADD DISK
    '/devices/diskc3' FORCE;
```

Replacing Disks in Disk Groups

A disk or multiple disks in a disk group can be replaced, rather than dropped and added back. The single replace operation is more efficient than dropping and adding disks. This operation is especially useful when disks are missing or damaged.

For example, you can issue the following statement to replace the `diskc7` disk with another disk identified by the `/devices/diskc18` path.

```
SQL> ALTER DISKGROUP data2 REPLACE DISK diskc7 WITH '/devices/diskc18' POWER 3;
```

The `power` option operates the same as the `power` option for the `ALTER DISKGROUP REBALANCE` statement, except that the `power` option cannot be set to 0. For information about the `power` option in rebalancing a disk group, refer to [“Manually Rebalancing Disk Groups”](#). For information about the `ASM_POWER_LIMIT` initialization parameter, refer to [“ASM_POWER_LIMIT”](#).

The `ALTER DISKGROUP SQL` statement with the `REPLACE` clause includes a `WAIT` or `NOWAIT` option, plus the `FORCE` option.

Renaming Disks in Disk Groups

You can rename a disk in a disk group with the `ALTER DISKGROUP RENAME DISK SQL` statement. In one SQL statement, you can rename one or multiple disks, or rename all disks in a disk group using the `RENAME DISKS ALL` clause.

For example, you can rename disks as follows:

```
SQL> ALTER DISKGROUP fra2 MOUNT RESTRICTED;
```

```
SQL> ALTER DISKGROUP fra2 RENAME DISK 'FRA1_0001' TO 'FRA2_0001',
    'FRA1_0002' TO 'FRA2_0002';
```

The `ALTER DISKGROUP diskgroupname RENAME DISKS ALL` statement can be run after the `renamedg` utility to change the names of the disks in the renamed disk group. For information about `renamedg`, refer to [“Renaming Disk Groups”](#).

When you run the `ALTER DISKGROUP diskgroupname RENAME DISKS ALL` statement, any disk name that is not in the format `diskgroupname_number` is

renamed to that format. Disk names that are already in the *diskgroupname_number* format are not changed.

You can only use the RENAME DISK operation when the disk group that contains the disk is in the MOUNT RESTRICTED state. If any disks in the disk group are offline, then the RENAME operation fails. If the new disk name exists, then the RENAME operation fails. You must have SYSASM privileges to rename a disk.

Dropping Disks from Disk Groups

To drop disks from a disk group, use the DROP DISK clause of the ALTER DISKGROUP statement. You can also drop all of the disks in specified failure groups using the DROP DISKS IN FAILGROUP clause.

When a disk is dropped, the disk group is rebalanced by moving all of the file extents from the dropped disk to other disks in the disk group. A drop disk operation might fail if not enough space is available on the other disks. The best approach is to perform both the add and drop operation with the same ALTER DISKGROUP statement. This has the benefit of rebalancing data extents only one time and ensuring that there is enough space for the rebalance operation to succeed.

Caution:

The ALTER DISKGROUP . . . DROP DISK SQL statement returns to SQL prompt before the drop and rebalance operations are complete. Do not reuse, remove, or disconnect the dropped disk until the HEADER_STATUS column for this disk in the V\$ASM_DISK view changes to FORMER. You can query the V\$ASM_OPERATION view to determine the amount of time remaining for the drop/rebalance operation to complete. For more information, refer to the *Oracle Database SQL Language Reference* and the *Oracle Database Reference*.

If you specify the FORCE clause for the drop operation, the disk is dropped even if Oracle ASM cannot read or write to the disk. You cannot use the FORCE flag when dropping a disk from an external redundancy disk group.

Caution:

A DROP FORCE operation leaves data at reduced redundancy until the subsequent rebalance operation completes. This increases your exposure to data loss if there is a subsequent disk failure during rebalancing. Use DROP FORCE with caution.

You can also drop disks from a disk group with ASMCA. Refer to [“Managing Disk Groups with ASMCA”](#).

The statements in [Example 6](#) demonstrate how to drop disks from the disk group data1 described in [“Using the ALTER DISKGROUP SQL Statement to Add Disks to a Disk Group”](#). The first example drops diska5 from disk group data1. The second example drops diska5 from disk group data1, and also illustrates how multiple actions are possible with one ALTER DISKGROUP statement.

Example 6 Dropping disks from disk groups

```
ALTER DISKGROUP data1 DROP DISK diska5;
```

```
ALTER DISKGROUP data1 DROP DISK diska5
      ADD FAILGROUP failgrp1 DISK '/devices/diska9' NAME diska9;
```

Intelligent Data Placement

Intelligent Data Placement enables you to specify disk regions on Oracle ASM disks for best performance. Using the disk region settings, you can ensure that frequently accessed data is placed on the outermost (hot) tracks which have greater speed and higher bandwidth. In addition, files with similar access patterns are located physically close, reducing latency. Intelligent Data Placement also enables the placement of primary and mirror extents into different hot or cold regions.

Intelligent Data Placement settings can be specified for a file or in disk group templates. The disk region settings can be modified after the disk group has been created. The disk region setting can improve I/O performance by placing more frequently accessed data in regions furthest from the spindle, while reducing your cost by increasing the usable space on a disk.

Intelligent Data Placement works best for the following:

- Databases with data files that are accessed at different rates. A database that accesses all data files in the same way is unlikely to benefit from Intelligent Data Placement.
- Disk groups that are more than 25% full. If the disk group is only 25% full, the management overhead is unlikely to be worth any benefit.
- Disks that have better performance at the beginning of the media relative to the end. Because Intelligent Data Placement leverages the geometry of the disk, it is well suited to JBOD (just a bunch of disks). In contrast, a storage array with LUNs composed of concatenated volumes masks the geometry from Oracle ASM.

The `COMPATIBLE.ASM` and `COMPATIBLE.RDBMS` disk group attributes must be set to 11.2 or higher to use Intelligent Data Placement.

Intelligent Data Placement can be managed with the `ALTER DISKGROUP ADD` or `MODIFY TEMPLATE SQL` statements and the `ALTER DISKGROUP MODIFY FILE SQL` statement.

- The `ALTER DISKGROUP TEMPLATE SQL` statement includes a disk region clause for setting *hot/mirrorhot* or *cold/mirrorcold* regions in a template:

```
ALTER DISKGROUP data ADD TEMPLATE datafile_hot
      ATTRIBUTE (
        HOT
        MIRRORHOT);
```

- The `ALTER DISKGROUP MODIFY FILE SQL` statement that sets disk region attributes for *hot/mirrorhot* or *cold/mirrorcold* regions:

```
ALTER DISKGROUP data MODIFY FILE '+data/orcl/datafile/users.259.679156903'
      ATTRIBUTE (
        HOT
        MIRRORHOT);
```

When you modify the disk region settings for a file, this action applies to new extensions of the file, but existing file contents are not affected until a rebalance operation. To apply the new Intelligent Data Placement policy for existing file contents, you can manually initiate a rebalance. A rebalance operation uses the last specified policy for the file extents. For information on the rebalance operation, see [“Manually Rebalancing Disk Groups”](#).

Oracle ASM Configuration Assistant (ASMCA) supports Intelligent Data Placement with template creation during disk group alterations. See [“Managing Disk Groups with ASMCA”](#).

To display information about Intelligent Data Placement regions, see [“Viewing Disk Region Information”](#) and [“iostat”](#).

Resizing Disks in Disk Groups

The `RESIZE` clause of `ALTER DISKGROUP` enables you to perform the following operations:

- Resize all disks in the disk group
- Resize specific disks
- Resize all of the disks in a specified failure group

If you do not specify a new size in the `SIZE` clause, then Oracle ASM uses the size of the disk as returned by the operating system. The new size is written to the Oracle ASM disk header and if the size of the disk is increasing, then the new space is immediately available for allocation. If the size is decreasing, rebalancing must relocate file extents beyond the new size limit to available space below the limit. If the rebalance operation can successfully relocate all extents, then the new size is made permanent, otherwise the rebalance fails.

The following example resizes all of the disks in failure group `failgrp1` of disk group `data1`. If the new size is greater than disk capacity, the statement fails.

Example 7 Resizing disks in disk groups

```
ALTER DISKGROUP data1
    RESIZE DISKS IN FAILGROUP failgrp1 SIZE 100G;
```

Undropping Disks in Disk Groups

The `UNDROP DISKS` clause of the `ALTER DISKGROUP` statement enables you to cancel all pending drops of disks within disk groups. If a drop disk operation has completed, then this statement cannot be used to restore it. This statement cannot be used to restore disks that are being dropped as the result of a `DROP DISKGROUP` statement, or for disks that are being dropped using the `FORCE` clause.

The following example cancels the dropping of disks from disk group `data1`:

Example 8 Undropping disks in disk groups

```
ALTER DISKGROUP data1 UNDROP DISKS;
```

Manually Rebalancing Disk Groups

You can manually rebalance the files in a disk group using the `REBALANCE` clause of the `ALTER DISKGROUP` statement. This would normally not be required, because Oracle ASM automatically rebalances disk groups when their configuration changes. You might want to do a manual rebalance operation to control the speed of what would otherwise be an automatic rebalance operation.

The `POWER` clause of the `ALTER DISKGROUP REBALANCE` statement specifies the degree of parallelism, and thus the speed of the rebalance operation. It can be set to a minimum value of 0 which halts a rebalancing operation until the statement is either

implicitly or explicitly rerun. A higher value increases the speed of the rebalance operation.

The default rebalance power is set by the `ASM_POWER_LIMIT` initialization parameter. The range of values for the `POWER` clause is the same for the `ASM_POWER_LIMIT` initialization parameter. For information about the `ASM_POWER_LIMIT` initialization parameter, refer to [“ASM_POWER_LIMIT”](#).

The power level of an ongoing rebalance operation can be changed by entering the rebalance statement with a new level.

The `ALTER DISKGROUP . . . REBALANCE` command by default returns immediately so that you can run other commands while the rebalance operation takes place asynchronously in the background. You can query the `V$ASM_OPERATION` view for the status of the rebalance operation.

To cause the `ALTER DISKGROUP . . . REBALANCE` command to wait until the rebalance operation is complete before returning, add the `WAIT` keyword to the `REBALANCE` clause. The wait functionality is especially useful in scripts. The command also accepts a `NOWAIT` keyword, which invokes the default behavior of conducting the rebalance operation asynchronously. You can interrupt a rebalance running in wait mode by typing `CTRL+C` on most platforms. This causes the command to return immediately with the message `ORA-01013: user requested cancel of current operation`, and then continue the rebalance operation asynchronously.

Additional rules for the rebalance operation include the following:

- An ongoing rebalance command is restarted if the storage configuration changes either when you alter the configuration, or if the configuration changes due to a failure or an outage. Furthermore, if the new rebalance fails because of a user error, then a manual rebalance may be required.
- The `ALTER DISKGROUP . . . REBALANCE` statement runs on a single node even if you are using Oracle Real Application Clusters (Oracle RAC).
- Oracle ASM can perform one disk group rebalance at a time on a given instance. If you have initiated multiple rebalances on different disk groups on a single node, then Oracle processes these operations in parallel on additional nodes if available; otherwise the rebalances are performed serially on the single node. You can explicitly initiate rebalances on different disk groups on different nodes in parallel.
- Rebalancing continues across a failure of the Oracle ASM instance performing the rebalance.
- The `REBALANCE` clause (with its associated `POWER` and `WAIT/NOWAIT` keywords) can also be used in `ALTER DISKGROUP` commands that add, drop, or resize disks.

Note:

Oracle restarts the processing of an ongoing rebalance operation if the storage configuration changes. If the next rebalance operation fails because of a user error, then a manual rebalance may be required.

The following example manually rebalances the disk group `data2`. The command does not return until the rebalance operation is complete.

For more information about rebalancing operations, refer to [“Tuning Rebalance Operations”](#).

Example 9 Manually rebalancing a disk group

```
ALTER DISKGROUP data2 REBALANCE POWER 5 WAIT;
```

Tuning Rebalance Operations

If the `POWER` clause is not specified in an `ALTER DISKGROUP` statement, or when rebalance is implicitly run by adding or dropping a disk, then the rebalance power defaults to the value of the `ASM_POWER_LIMIT` initialization parameter. You can adjust the value of this parameter dynamically. The range of values for the `POWER` clause is the same for the `ASM_POWER_LIMIT` initialization parameter. For information about the `ASM_POWER_LIMIT` initialization parameter, refer to [“ASM_POWER_LIMIT”](#).

The higher the power limit, the more quickly a rebalance operation can complete. Rebalancing takes longer with lower power values, but consumes fewer processing and I/O resources which are shared by other applications, such as the database.

Oracle ASM tries to keep a rebalance I/O for each unit of power. Each I/O requires PGA memory for the extent involved in the relocation.

The default value of 1 minimizes disruption to other applications. The appropriate value is dependent on your hardware configuration, performance requirements, and availability requirements. Oracle ASM always adjusts the power to fit available memory.

When the `COMPATIBLE .ASM` disk group is set to 11.2.0.2 or higher, the rebalance operation may be run as one process using asynchronous I/O. You can check the Oracle ASM alert log for details on the rebalance process.

If a rebalance is in progress because a disk is manually or automatically dropped, then increasing the power of the rebalance shortens the time frame during which redundant copies of that data on the dropped disk are reconstructed on other disks.

You can also affect rebalance behavior with the `CONTENT .CHECK` and `THIN_PROVISIONED` disk group attributes. For information about disk group attributes, refer to [“Summary of Disk Group Attributes”](#).

The `EXPLAIN WORK SQL` statement determines the amount of work for a rebalance operation and the resulting calculations are displayed in the `V$ASM_ESTIMATE` view.

For example:

```
EXPLAIN WORK FOR ALTER DISKGROUP data DROP DISK data_0000;
Explained.
```

```
SELECT est_work FROM V$ASM_ESTIMATE;
EST_WORK
-----
      4211
```

```
EXPLAIN WORK SET STATEMENT_ID='online' FOR ALTER DISKGROUP data
  ONLINE disk data_000;
Explained.
```

```
SELECT est_work FROM V$ASM_ESTIMATE WHERE STATEMENT_ID='online';
EST_WORK
-----
      421
```

The `V$ASM_ESTIMATE` view provides information for adjusting `ASM_POWER_LIMIT` and the resulting power of rebalance operations. The `EST_WORK` column provides an estimate of the number of allocation units that have to be moved by the rebalance operation to complete.

The PASS column of V\$ASM_OPERATION is updated for resync and rebalance operations. The contents of the column can be RESYNC, REBALANCE, or COMPACT. For example, the following SQL query shows values in the PASS column during a rebalance operation.

```
SQL> SELECT GROUP_NUMBER, PASS, STATE FROM V$ASM_OPERATION;
```

GROUP_NUMBER	PASS	STAT
2	RESYNC	WAIT
2	REBALANCE	WAIT
2	COMPACT	WAIT

For more information about rebalancing disk groups, refer to [“Manually Rebalancing Disk Groups”](#).

Scrubbing Disk Groups

Oracle ASM disk scrubbing improves availability and reliability by searching for data that may be less likely to be read. Disk scrubbing checks logical data corruptions and repairs them automatically in normal and high redundancy disks groups. The scrubbing process repairs logical corruptions using the mirror disks. Disk scrubbing can be combined with disk group rebalancing to reduce I/O resources. The disk scrubbing process has minimal impact to the regular I/O in production systems.

You can perform scrubbing on a disk group, a specified disk, or a specified file of a disk group with the ALTER DISKGROUP SQL statement. For example, the following SQL statements show various options used when running the ALTER DISKGROUP *disk_group* SCRUB SQL statement.

```
SQL> ALTER DISKGROUP data SCRUB POWER LOW;
```

```
SQL> ALTER DISKGROUP data SCRUB FILE '+DATA/ORCL/DATAFILE/example.
266.806582193'
      REPAIR POWER HIGH FORCE;
```

```
SQL> ALTER DISKGROUP data SCRUB DISK DATA_0005 REPAIR POWER HIGH FORCE;
```

When using ALTER DISKGROUP with the SCRUB option, the following items apply:

- The optional REPAIR option automatically repairs disk corruptions. If the REPAIR option is not specified, then the SCRUB option only checks and reports logical corruptions of the specified target.
- The optional POWER value can be set to AUTO, LOW, HIGH, or MAX. If the POWER option is not specified, the power value defaults to AUTO and the power adjusts to the optimum level for the system.
- If the optional WAIT option is specified, the command returns after the scrubbing operation has completed. If the WAIT option is not specified, the scrubbing operation is added into the scrubbing queue and the command returns immediately.
- If the optional FORCE option is specified, the command is processed even if the system I/O load is high or scrubbing has been disabled internally at the system level.

The scrubbing process is visible in the fields of the V\$ASM_OPERATION view while the scrubbing process is running.

Oracle ASM Disk Discovery

Disk discovery is the mechanism used to find the operating system names for disks Oracle ASM can access. This mechanism finds all the disks that comprise a disk group to be mounted, the disks an administrator wants to add to a disk group, or the disks the administrator might consider adding to a disk group. This section contains the following topics:

- [How A Disk is Discovered](#)
- [Disk Discovery Rules](#)
- [Improving Disk Discovery Time](#)

For additional information about disk discovery and the `ASM_DISKSTRING` initialization parameter, refer to “[ASM_DISKSTRING](#)”.

How A Disk is Discovered

When an Oracle ASM instance is initialized, Oracle ASM discovers and examines the contents of all of the disks that are in the paths that you designated with values in the `ASM_DISKSTRING` initialization parameter.

Disk discovery also occurs when you:

- Run the following SQL statements
 - Mount a disk group with `ALTER DISKGROUP MOUNT`
 - Online a disk with `ALTER DISKGROUP ONLINE DISK`
 - Add a disk to a disk group with `CREATE` or `ALTER DISKGROUP...ADD DISK`
 - Resize a disk in a disk group with `ALTER DISKGROUP...RESIZE DISK`
 - Query with `SELECT FROM V$ASM_DISKGROUP` or `V$ASM_DISK` views
- Run Oracle ASM Configuration Assistant (ASMCA) operations or `ASMCMD` commands that perform the same operations as the SQL statements previously listed

After Oracle ASM successfully discovers a disk, the disk appears in the `V$ASM_DISK` view. Disks that belong to a disk group, that is, disks that have a disk group name in the disk header, show a header status of `MEMBER`. Disks that were discovered, but that have not yet been assigned to a disk group, have a status of either `CANDIDATE` or `PROVISIONED`. Disks that previously belonged to a disk group and were dropped cleanly from the disk group have a status of `FORMER`.

The `PROVISIONED` status implies that an additional platform-specific action has been taken by an administrator to make the disk available for Oracle ASM. For example, on Windows computers, the administrator might have used `asmtool` or `asmtoolg` to stamp the disk with a header. For example, on Linux computers, the administrator might have used Oracle ASM Filter Driver or `ASMLIB` to prepare the disk for Oracle ASM.

[Example 10](#) shows a SQL query on `V$ASM_DISK` that displays the header status of a group of disks.

See Also:

Oracle Database Reference for information about the header status of an Oracle ASM disk that is displayed in the V\$ASM_DISK view

Example 10 Querying V\$ASM_DISK for header status

```
SQL> SELECT name, header_status, path FROM V$ASM_DISK
       WHERE path LIKE '/devices/disk0%';
```

NAME	HEADER_STATUS	PATH
	FORMER	/devices/disk02
	FORMER	/devices/disk01
	CANDIDATE	/devices/disk07
DISK06	MEMBER	/devices/disk06
DISK05	MEMBER	/devices/disk05
DISK04	MEMBER	/devices/disk04
DISK03	MEMBER	/devices/disk03

7 rows selected.

Disk Discovery Rules

The rules for discovering Oracle ASM disks are as follows:

- Oracle ASM can discover up to 10,000 disks. That is, if more than 10,000 disks match the ASM_DISKSTRING initialization parameter, then Oracle ASM discovers only the first 10,000.
- Oracle ASM only discovers disk partitions. Oracle ASM does not discover partitions that include the partition table.
- From the perspective of the installation, candidate disks are those that have the CANDIDATE, PROVISIONED, or FORMER header status. These disks with a CANDIDATE, PROVISIONED, or FORMER status can be added to Oracle ASM disk groups without using the FORCE flag.
- When adding a disk, the FORCE option must be used if Oracle ASM recognizes that the disk was managed by Oracle. Such a disk appears in the V\$ASM_DISK view with a status of FOREIGN. In this case, you can only add the disk to a disk group by using the FORCE keyword.
- MEMBER disks can usually be added to a disk group by specifying the FORCE flag, if the disks are not part of a currently mounted disk group.

In addition, Oracle ASM identifies the following configuration errors during discovery:

- Multiple paths to the same disk

In this case, if the disk is part of a disk group, then disk group mount fails. If the disk is being added to a disk group with the ADD DISK or CREATE DISKGROUP command, then the command fails. To correct the error, adjust the ASM_DISKSTRING value so that Oracle ASM does not discover multiple paths to the same disk. Or if you are using multipathing software, then ensure that you include only the pseudo-device name in the ASM_DISKSTRING value. See [“Oracle ASM and Multipathing”](#).
- Multiple Oracle ASM disks with the same disk header

This can be caused by having copied one disk onto another. In this case, the disk group mount operation fails.

Improving Disk Discovery Time

The value for the `ASM_DISKSTRING` initialization parameter is an operating system-dependent value that Oracle ASM uses to limit the set of paths that the discovery process uses to search for disks. When a new disk is added to a disk group, each Oracle ASM instance that has the disk group mounted must be able to discover the new disk using its `ASM_DISKSTRING`.

In many cases, the default value (`NULL`) is sufficient. Using a more restrictive value might reduce the time required for Oracle ASM to perform discovery, and thus improve disk group mount time or the time for adding a disk to a disk group. Oracle may dynamically change the `ASM_DISKSTRING` before adding a disk so that the new disk is discovered through this parameter.

The default value of `ASM_DISKSTRING` might not find all disks in all situations. If your site is using Oracle ASM Filter Driver or a third-party vendor, then you may have discovery string conventions that you must use for `ASM_DISKSTRING`. For information about Oracle ASM Filter Driver, refer to [“Oracle ASM Filter Driver”](#).

In addition, if your installation uses multipathing software, then the software might place pseudo-devices in a path that is different from the operating system default. See [“Oracle ASM and Multipathing”](#) and consult the multipathing vendor documentation for details.

Managing Capacity in Disk Groups

When Oracle ASM provides redundancy, such as when you create a disk group with `NORMAL` or `HIGH` redundancy, you must have sufficient capacity in each disk group to manage a re-creation of data that is lost after a failure of one or two failure groups. After one or more disks fail, the process of restoring redundancy for all data requires space from the surviving disks in the disk group. If not enough space remains, then some files might end up with reduced redundancy.

Reduced redundancy means that one or more extents in the file are not mirrored at the expected level. For example, a reduced redundancy file in a high redundancy disk group has at least one file extent with two or fewer total copies of the extent instead of three. For unprotected files, data extents could be completely missing. Other causes of reduced redundancy files are disks running out of space or an insufficient number of failure groups. The `REDUNDANCY_LOWERED` column in the `V$ASM_FILE` view provides information about files with reduced redundancy.

The following guidelines help ensure that you have sufficient space to restore full redundancy for all disk group data after the failure of one or more disks.

- Normal redundancy disk group - It is best to have enough free space in your disk group to tolerate the loss of all disks in one failure group. The amount of free space should be equivalent to the size of the largest failure group.
- High redundancy disk group - It is best to have enough free space to cope with the loss of all disks in two failure groups. The amount of free space should be equivalent to the sum of the sizes of the two largest failure groups.

Note:

When you lose multiple disks from multiple failure groups, then you could lose both the primary and the redundant copies of your data. In addition, if you do not have enough capacity to restore redundancy, then Oracle ASM can continue to operate. However, if another disk fails, then the system may not be able to tolerate additional failures.

The `V$ASM_DISKGROUP` view contains the following columns that contain information to help you manage capacity:

- `REQUIRED_MIRROR_FREE_MB` indicates the amount of space that must be available in a disk group to restore full redundancy after the worst failure that can be tolerated by the disk group without adding additional storage. This requirement ensures that there are sufficient failure groups to restore redundancy. Also, this worst failure refers to a permanent failure where the disks must be dropped, not the case where the disks go offline and then back online.

The amount of space displayed in this column takes the effects of mirroring into account. The value is computed as follows:

- A normal redundancy disk group with more than two `REGULAR` failure groups
The value is the total raw space for all of the disks in the largest failure group. The largest failure group is the one with the largest total raw capacity. For example, if each disk is in its own failure group, then the value would be the size of the largest capacity disk.
- A high redundancy disk group with more than three `REGULAR` failure groups
The value is the total raw space for all of the disks in the two largest failure groups.

See Also:

Oracle Exadata documentation for information about calculating `REQUIRED_MIRROR_FREE_MB` on Oracle Exadata systems.

Oracle Database Appliance documentation for information about calculating `REQUIRED_MIRROR_FREE_MB` on Oracle Database Appliance systems.

- `USABLE_FILE_MB` indicates the amount of free space, adjusted for mirroring, that is available for new files to restore redundancy after a disk failure. `USABLE_FILE_MB` is computed by subtracting `REQUIRED_MIRROR_FREE_MB` from the total free space in the disk group and then adjusting the value for mirroring. For example, in a normal redundancy disk group where by default the mirrored files use disk space equal to twice their size, if 4 GB of actual usable file space remains, then `USABLE_FILE_MB` equals roughly 2 GB. You can then add a file that is up to 2 GB. For information about negative values of `USABLE_FILE_MB`, refer to [“Negative Values of USABLE_FILE_MB”](#).
- `TOTAL_MB` is the total usable capacity of a disk group in megabytes. The calculations for data in this column take the disk header overhead into consideration. The disk header overhead depends on the number of Oracle ASM disks and Oracle ASM files. This value is typically about 1% of the total raw storage

capacity. For example, if the total LUN capacity provisioned for Oracle ASM is 100 GB, then the value in the `TOTAL_MB` column would be about 99 GB.

- `FREE_MB` is the unused capacity of the disk group in megabytes, without considering any data imbalance. There may be situations where the value in the `FREE_MB` column shows unused capacity but because one Oracle ASM disk is full, database writes fail because of the imbalance in the disk group. Ensure that you initiate a manual rebalance to force even data distribution which results in an accurate presentation of the values in the `FREE_MB` column.

With fine grain striping using 128 KB, the storage is preallocated to be eight times the AU size. The data file size may appear slightly larger on Oracle ASM than on a local file system because of the preallocation.

When you use Oracle ASM normal or high redundancy, the disk space utilization becomes more complex to measure because it depends on several variables.

Note:

The values in the `TOTAL_MB` and `FREE_MB` columns best describe space usage when you do not configure Oracle ASM mirroring, that is, when you use external redundancy.

The results from the following query show capacity metrics for a normal redundancy disk group that consists of six 1 GB (1024 MB) disks, each in its own failure group:

```
SQL> SELECT name, type, total_mb, free_mb, required_mirror_free_mb,
         usable_file_mb FROM V$ASM_DISKGROUP;
```

NAME	TYPE	TOTAL_MB	FREE_MB	REQUIRED_MIRROR_FREE_MB	USABLE_FILE_MB
DATA	NORMAL	6144	3768	1024	1372

The `REQUIRED_MIRROR_FREE_MB` column shows that 1 GB of extra capacity must be available to restore full redundancy after one or more disks fail. The first three numeric columns in the query results are raw numbers. That is, they do not take redundancy into account. Only the last column is adjusted for normal redundancy. In the query output example for the data disk group, the calculation is as follows:

$$(\text{FREE_MB} - \text{REQUIRED_MIRROR_FREE_MB}) / 2 = \text{USABLE_FILE_MB}$$

$$(3768 - 1024) / 2 = 2744 / 2 = 1372$$

Negative Values of `USABLE_FILE_MB`

Due to the relationship between `FREE_MB`, `REQUIRED_MIRROR_FREE_MB`, and `USABLE_FILE_MB`, `USABLE_FILE_MB` can become negative. Although this is not necessarily a critical situation, it does mean that:

- Depending on the value of `FREE_MB`, you may not be able to create new files.
- The next failure might result in files with reduced redundancy.

If `USABLE_FILE_MB` becomes negative, it is strongly recommended that you add more space to the disk group as soon as possible.

Oracle ASM Mirroring and Disk Group Redundancy

This section contains the following topics:

- [Mirroring_ Redundancy_ and Failure Group Options](#)
- [Oracle ASM Recovery from Read and Write I/O Errors](#)
- [Oracle ASM Fast Mirror Resync](#)
- [Even Read for Disk Groups](#)
- [Preferred Read Failure Groups](#)

Mirroring, Redundancy, and Failure Group Options

If you specify mirroring for a file, then Oracle ASM automatically stores redundant copies of the file extents in separate failure groups. Failure groups apply only to normal and high redundancy disk groups. You can define the failure groups for each disk group when you create or alter the disk group.

There are three types of disk groups based on the Oracle ASM redundancy level. [Table 1](#) lists the types with their supported and default mirroring levels. The default mirroring levels indicate the mirroring level with which each file is created unless a different mirroring level is designated.

Table 1 *Mirroring options for Oracle ASM disk group types*

Disk Group Type	Supported Mirroring Levels	Default Mirroring Level
External redundancy	Unprotected (none)	Unprotected
Normal redundancy	Two-way, three-way, unprotected (none)	Two-way
High redundancy	Three-way	Three-way

The redundancy level controls how many disk failures are tolerated without dismounting the disk group or losing data. Each file is allocated based on its own redundancy, but the default comes from the disk group.

The redundancy levels are:

- External redundancy

Oracle ASM does not provide mirroring redundancy and relies on the storage system to provide RAID functionality. Any write error causes a forced dismount of the disk group. All disks must be located to successfully mount the disk group.
- Normal redundancy

Oracle ASM provides two-way mirroring by default, which means that all files are mirrored so that there are two copies of every [extent](#). A loss of one Oracle ASM disk is tolerated. You can optionally choose three-way or unprotected mirroring.

A file specified with HIGH redundancy (three-way mirroring) in a NORMAL redundancy disk group provides additional protection from a bad disk sector, not protection from a disk failure.
- High redundancy

Oracle ASM provides triple mirroring by default. A loss of two Oracle ASM disks in different failure groups is tolerated.

If there are not enough online failure groups to satisfy the file mirroring (redundancy attribute value) specified in the disk group file type template, Oracle ASM allocates as many mirrors copies as possible and subsequently allocates the remaining mirrors

when sufficient online failure groups are available. For information about specifying Oracle ASM disk group templates, see [“Managing Disk Group Templates”](#).

Failure groups enable the mirroring of metadata and user data. System reliability can diminish if your environment has an insufficient number of failure groups.

This section contains these topics:

- [Oracle ASM Failure Groups](#)
- [How Oracle ASM Manages Disk Failures](#)
- [Guidelines for Using Failure Groups](#)
- [Failure Group Frequently Asked Questions](#)

Oracle ASM Failure Groups

Failure groups are used to store mirror copies of data. When Oracle ASM allocates an extent for a normal redundancy file, Oracle ASM allocates a primary copy and a secondary copy. Oracle ASM chooses the disk on which to store the secondary copy so that it is in a different failure group than the primary copy. Each copy is on a disk in a different failure group so that the simultaneous failure of all disks in a failure group does not result in data loss.

A failure group is a subset of the disks in a disk group, which could fail at the same time because they share hardware. The failure of common hardware must be tolerated. Four drives that are in a single removable tray of a large JBOD (Just a Bunch of Disks) array should be in the same failure group because the tray could be removed making all four drives fail at the same time. Drives in the same cabinet could be in multiple failure groups if the cabinet has redundant power and cooling so that it is not necessary to protect against failure of the entire cabinet. However, Oracle ASM mirroring is not intended to protect against a fire in the computer room that destroys the entire cabinet.

There are always failure groups even if they are not explicitly created. If you do not specify a failure group for a disk, then Oracle automatically creates a new failure group containing just that disk, except for disk groups containing disks on Oracle Exadata cells.

A normal redundancy disk group must contain at least two failure groups. A high redundancy disk group must contain at least three failure groups. However, Oracle recommends using more failure groups. A small number of failure groups, or failure groups of uneven capacity, can create allocation problems that prevent full use of all of the available storage.

Oracle recommends a minimum of three failure groups for normal redundancy disk groups and five failure groups for high redundancy disk groups to maintain the necessary number of copies of the Partner Status Table (PST) and to ensure robustness with respect to storage hardware failures.

In the event of a system failure, three failure groups in a normal redundancy disk group allow a comparison among three PSTs to accurately determine the most up to date and correct version of the PST, which could not be done with a comparison between only two PSTs. Similarly with a high redundancy disk group, if two failure groups are offline, then Oracle ASM would be able to make a comparison among the three remaining PSTs.

If configuring an extra failure group presents a problem with storage capacity management, then a quorum failure group can be used as the extra failure group to

store a copy of the PST. A quorum failure group does not require the same capacity as the other failure groups.

Failure groups can be specified as regular or quorum failure groups. For information about quorum failure groups, see [“Storing Oracle Cluster Registry and Voting Files in Oracle ASM Disk Groups”](#).

See Also:

Oracle Exadata documentation for information about Oracle Exadata failure groups

How Oracle ASM Manages Disk Failures

Depending on the redundancy level of a disk group and how you define failure groups, the failure of one or more disks could result in either of the following:

- The disks are first taken offline and then automatically dropped. In this case, the disk group remains mounted and serviceable. In addition, because of mirroring, all of the disk group data remains accessible. After the disk drop operation, Oracle ASM performs a rebalance to restore full redundancy for the data on the failed disks.
- The entire disk group is automatically dismounted, which means loss of data accessibility.

Guidelines for Using Failure Groups

The following are guidelines for using failure groups:

- Each disk in a disk group can belong to only one failure group.
- Failure groups should all be of the same size. Failure groups of different sizes may lead to reduced availability.
- Oracle ASM requires at least two failure groups to create a normal redundancy disk group and at least three failure groups to create a high redundancy disk group.

Failure Group Frequently Asked Questions

This section discusses frequently asked questions about failure group under the following topics:

- [How Many Failure Groups Should I Create?](#)
- [How are Multiple Failure Groups Recovered after Simultaneous Failures?](#)
- [When Should External, Normal, or High Redundancy Be Used?](#)

How Many Failure Groups Should I Create?

Choosing the number of failure groups to create depends on the types of failures that must be tolerated without data loss. For small numbers of disks, such as fewer than 20, it is usually best to use the default failure group creation that puts every disk in its own failure group.

Using the default failure group creation for small numbers of disks is also applicable for large numbers of disks where your main concern is disk failure. For example, a

disk group might be configured from several small modular disk arrays. If the system must continue operating when an entire modular array fails, then a failure group should consist of all of the disks in one module. If one module fails, then all of the data on that module is relocated to other modules to restore redundancy. Disks should be placed in the same failure group if they depend on a common piece of hardware whose failure must be tolerated with no loss of availability.

How are Multiple Failure Groups Recovered after Simultaneous Failures?

A simultaneous failure can occur if there is a failure of a piece of hardware used by multiple failure groups. This type of failure usually forces a dismount of the disk group if all disks are unavailable.

When Should External, Normal, or High Redundancy Be Used?

Oracle ASM mirroring runs on the database server and Oracle recommends to off load this processing to the storage hardware RAID controller by using external redundancy. You can use normal redundancy in the following scenarios:

- Storage system does not have RAID controller
- Mirroring across storage arrays
- Extended cluster configurations

In general, Oracle ASM mirroring is the Oracle alternative to third party logical volume managers. Oracle ASM mirroring eliminates the deployment of additional layers of software complexity in your Oracle Database environment.

Oracle ASM Recovery from Read and Write I/O Errors

Read errors can be the result of a loss of access to the entire disk or media corruptions on an otherwise a healthy disk. Oracle ASM tries to recover from read errors on corrupted sectors on a disk. When a read error by the database or Oracle ASM triggers the Oracle ASM instance to attempt bad block remapping, Oracle ASM reads a good copy of the extent and copies it to the disk that had the read error.

- If the write to the same location succeeds, then the underlying allocation unit (sector) is deemed healthy. This might be because the underlying disk did its own bad block reallocation.
- If the write fails, Oracle ASM attempts to write the extent to a new allocation unit on the same disk. If this write succeeds, the original allocation unit is marked as unusable. If the write fails, the disk is taken offline.

One unique benefit on Oracle ASM based mirroring is that the database instance is aware of the mirroring. For many types of logical corruptions such as a bad checksum or incorrect System Change Number (SCN), the database instance proceeds through the mirror side looking for valid content and proceeds without errors. If the process in the database that encountered the read can obtain the appropriate locks to ensure data consistency, it writes the correct data to all mirror sides.

When encountering a write error, a database instance sends the Oracle ASM instance a *disk offline* message.

- If database can successfully complete a write to at least one extent copy and receive acknowledgment of the offline disk from Oracle ASM, the write is considered successful.

- If the write to all mirror side fails, database takes the appropriate actions in response to a write error such as taking the tablespace offline.

When the Oracle ASM instance receives a write error message from a database instance or when an Oracle ASM instance encounters a write error itself, the Oracle ASM instance attempts to take the disk offline. Oracle ASM consults the Partner Status Table (PST) to see whether any of the disk's partners are offline. If too many partners are offline, Oracle ASM forces the dismounting of the disk group. Otherwise, Oracle ASM takes the disk offline.

The ASMCMD `remap` command was introduced to address situations where a range of bad sectors exists on a disk and must be corrected before Oracle ASM or database I/O. For information about the `remap` command, see "[remap](#)".

Oracle ASM Fast Mirror Resync

Restoring the redundancy of an Oracle ASM disk group after a transient disk path failure can be time consuming. This is especially true if the recovery process requires rebuilding an entire Oracle ASM disk group. Oracle ASM fast mirror resync significantly reduces the time to resynchronize a failed disk in such situations. When you replace the failed disk, Oracle ASM can quickly resynchronize the Oracle ASM disk extents.

Note:

To use this feature, the disk group compatibility attributes must be set to 11.1 or higher. For more information, refer to "[Disk Group Compatibility](#)".

Any problems that make a failure group temporarily unavailable are considered transient failures that can be recovered by the Oracle ASM fast mirror resync feature. For example, transient failures can be caused by disk path malfunctions, such as cable failures, host bus adapter failures, controller failures, or disk power supply interruptions.

Oracle ASM fast resync keeps track of pending changes to extents on an offline disk during an outage. The extents are resynced when the disk is brought back online.

By default, Oracle ASM drops a disk in 3.6 hours after it is taken offline. You can set the `DISK_REPAIR_TIME` disk group attribute to delay the drop operation by specifying a time interval to repair the disk and bring it back online. The time can be specified in units of minutes (m or M) or hours (h or H). If you omit the unit, then the default unit is hours. The `DISK_REPAIR_TIME` disk group attribute can only be set with the `ALTER DISKGROUP` SQL statement and is only applicable to normal and high redundancy disk groups.

If the attribute is not set explicitly, then the default value (3.6h) applies to disks that have been set to `OFFLINE` mode without an explicit `DROP AFTER` clause. Disks taken offline due to I/O errors do not have a `DROP AFTER` clause.

The default `DISK_REPAIR_TIME` attribute value is an estimate that should be adequate for most environments. However, ensure that the attribute value is set to the amount of time that you think is necessary in your environment to fix any transient disk error, and during which you are able to tolerate reduced data redundancy.

The elapsed time (since the disk was set to `OFFLINE` mode) is incremented only when the disk group containing the offline disks is mounted. The `REPAIR_TIMER` column of `V$ASM_DISK` shows the amount of time left (in seconds) before an offline disk is

dropped. After the specified time has elapsed, Oracle ASM drops the disk. You can override this attribute with the `ALTER DISKGROUP OFFLINE DISK` statement and the `DROP AFTER` clause.

Note:

If a disk is offlined by Oracle ASM because of an I/O (write) error or is explicitly offlined using the `ALTER DISKGROUP... OFFLINE` statement without the `DROP AFTER` clause, then the value specified for the `DISK_REPAIR_TIME` attribute for the disk group is used.

Altering the `DISK_REPAIR_TIME` attribute has no effect on offline disks. The new value is used for any disks that go offline after the attribute is updated. You can confirm this behavior by viewing the Oracle ASM alert log.

If an offline disk is taken offline for a second time, then the elapsed time is reset and restarted. If another time is specified with the `DROP AFTER` clause for this disk, the first value is overridden and the new value applies. A disk that is in `OFFLINE` mode cannot be dropped with an `ALTER DISKGROUP DROP DISK` statement; an error is returned if attempted. If for some reason the disk must be dropped (such as the disk cannot be repaired) before the repair time has expired, a disk can be dropped immediately by issuing a second `OFFLINE` statement with a `DROP AFTER` clause specifying `0h` or `0m`.

You can use `ALTER DISKGROUP` to set the `DISK_REPAIR_TIME` attribute to a specified hour or minute value, such as 4.5 hours or 270 minutes. For example:

```
ALTER DISKGROUP data SET ATTRIBUTE 'disk_repair_time' = '4.5h'
ALTER DISKGROUP data SET ATTRIBUTE 'disk_repair_time' = '270m'
```

After you repair the disk, run the SQL statement `ALTER DISKGROUP ONLINE DISK`. This statement brings a repaired disk group back online to enable writes so that no new writes are missed. This statement also starts a procedure to copy of all of the extents that are marked as stale on their redundant copies.

If a disk goes offline when the Oracle ASM instance is in rolling upgrade mode, the disk remains offline until the rolling upgrade has ended and the timer for dropping the disk is stopped until the Oracle ASM cluster is out of rolling upgrade mode. See [“Upgrading and Patching Oracle ASM”](#). Examples of taking disks offline and bringing them online follow.

The following example takes disk `DATA_001` offline and drops it after five minutes.

```
ALTER DISKGROUP data OFFLINE DISK DATA_001 DROP AFTER 5m;
```

The next example takes the disk `DATA_001` offline and drops it after the time period designated by `DISK_REPAIR_TIME` elapses:

```
ALTER DISKGROUP data OFFLINE DISK DATA_001;
```

This example takes all of the disks in failure group `FG2` offline and drops them after the time period designated by `DISK_REPAIR_TIME` elapses. If you used a `DROP AFTER` clause, then the disks would be dropped after the specified time:

```
ALTER DISKGROUP data OFFLINE DISKS IN FAILGROUP FG2;
```

The next example brings all of the disks in failure group `FG2` online:

```
ALTER DISKGROUP data ONLINE DISKS IN FAILGROUP FG2;
```

This example brings only disk DATA_001 online:

```
ALTER DISKGROUP data ONLINE DISK DATA_001;
```

This example brings all of the disks in disk group DATA online:

```
ALTER DISKGROUP data ONLINE ALL;
```

Querying the V\$ASM_OPERATION view while you run ALTER DISKGROUP ONLINE statements displays the name and state of the current operation that you are performing. For example, the following SQL query shows values in the PASS column during an online operation.

```
SQL> SELECT GROUP_NUMBER, PASS, STATE FROM V$ASM_OPERATION;
```

GROUP_NUMBER	PASS	STAT
1	RESYNC	RUN
1	REBALANCE	WAIT
1	COMPACT	WAIT

An offline operation does not generate a display in a V\$ASM_OPERATION view query.

You can set the FAILGROUP_REPAIR_TIME and CONTENT .TYPE disk group attributes. The FAILGROUP_REPAIR_TIME disk group attribute specifies a default repair time for the failure groups in the disk group. The CONTENT .TYPE disk group attribute specifies the type of data expected to be stored in a disk group. You can set these attributes with ASMCA, ASMCMD mkdrg, or SQL CREATE and ALTER DISKGROUP statements. For information about disk group attributes, refer to [“Managing Disk Group Attributes”](#).

The ASMCMD lstop command shows the resync time estimate. There are separate rows in the V\$ASM_OPERATION table for different phases of rebalance: disk resync, rebalance, and data compaction.

The ASMCMD online command has a power option to specify the power for the online operation. The SQL ALTER DISKGROUP REPLACE DISK statement also has the power option.

The ASMCMD chdrg command provides the replace option in addition to the add and drop tags. The ASMCMD mkdrg command has an additional time parameter (-t) to specify the time to offline a failure group.

See Also:

Oracle Database SQL Language Reference for information about ALTER DISKGROUP and CREATE DISKGROUP

Even Read for Disk Groups

The Even Read feature distributes data reads evenly across all the disks in a disk group. For each I/O request presented to the system, there may be one or more disks that contain the data. With this feature, each request to read can be sent to the least loaded of the possible source disks.

The Even Read functionality is enabled by default on all Oracle Database and Oracle ASM instances of version 12.1 and higher in non-Exadata environments. The functionality is enabled in an Exadata environment when there is a failure.

Preferred Read Failure Groups

When you configure Oracle ASM failure groups, it might be more efficient for a node to read from an extent that is closest to the node, even if that extent is a secondary extent. In other words, you can configure Oracle ASM to read from a secondary extent if that extent is closer to the node instead of Oracle ASM reading from the primary copy which might be farther from the node. Using the preferred read failure groups feature is most useful in extended clusters.

To use this feature, Oracle recommends that you configure at least one mirrored extent copy from a disk that is local to a node in an extended cluster. However, a failure group that is preferred for one instance might be remote to another instance in the same Oracle RAC database. The parameter setting for preferred read failure groups is instance specific. For information about configuring preferred read failure groups, refer to [“Configuring and Administering Preferred Read Failure Groups”](#).

Both the Oracle ASM clients and Oracle ASM require Oracle Database 11g Release 1 (11.1) or higher to use preferred read failure groups.

Note:

If you do not specify failure groups for a disk group, each disk in the disk group belongs to its own failure group. Oracle does not recommend that you configure multiple preferred read failure groups in a disk group for an Oracle ASM instance. For any given instance, if you specify multiple failure groups in the same disk group as preferred read, a warning message is written to the alert log.

See Also:

Oracle Real Application Clusters Administration and Deployment Guide for information about configuring preferred read disks in extended clusters

Configuring and Administering Preferred Read Failure Groups

To configure this feature, set the `ASM_PREFERRED_READ_FAILURE_GROUPS` initialization parameter to specify a list of failure group names as preferred read disks. For more information about this initialization parameter, refer to [“ASM_PREFERRED_READ_FAILURE_GROUPS”](#).

Set the parameter where *diskgroup* is the name of the disk group and *failuregroup* is the name of the failure group, separating these variables with a period. Oracle ASM ignores the name of a failure group that you use in this parameter setting if the failure group does not exist in the named disk group. You can append multiple values using commas as a separator as follows:

```
ASM_PREFERRED_READ_FAILURE_GROUPS = diskgroup.failuregroup,...
```

In an extended cluster, the failure groups that you specify with settings for the `ASM_PREFERRED_READ_FAILURE_GROUPS` parameter should only contain disks that are local to the instance. For normal redundancy disk groups, there should be only one failure group on each site of the extended cluster.

If there are multiple mirrored copies and you have set a value for the `ASM_PREFERRED_READ_FAILURE_GROUPS` parameter, then Oracle ASM first reads

the copy that resides on a preferred read disk. If that read fails, then Oracle ASM attempts to read from the next mirrored copy that might not be on a preferred read disk.

Having multiple failure groups on one site can cause the loss of access to the disk group by the other sites if the site containing multiple failure groups fails. In addition, by having multiple failure groups on a site, an extent might not be mirrored to another site. This can diminish the read performance of the failure group on the other site.

For example, for a normal redundancy disk group, if a site contains two failure groups of a disk group, then Oracle ASM might put both mirror copies of an extent on the same site. In this configuration, Oracle ASM cannot protect against data loss from a site failure.

You should configure at most two failure groups on a site for a high redundancy disk group. If there are three sites in an extended cluster, for the same reason previously mentioned, then you should only create one failure group.

For a two-site extended cluster, a normal redundancy disk group only has two failure groups. In this case, you can only specify one failure group as a preferred read failure group for each instance.

You can use views to identify preferred read failure groups, such as the `V$ASM_DISK` view that shows whether a disk is a preferred read disk by the value in the `PREFERRED_READ` column. You can also use `V$ASM_DISK` to verify whether local disks in an extended cluster are preferred read disks. Use the Oracle ASM disk I/O statistics to verify that read operations are using the preferred read disks that you configured.

If a disk group is not optimally configured for an extended cluster, then Oracle ASM records warning messages in the alert logs. To identify specific performance issues with Oracle ASM preferred read failure groups, use the `V$ASM_DISK_IOSTAT` view. This view displays disk I/O statistics for each Oracle ASM client. You can also query the `V$ASM_DISK_IOSTAT` view on a database instance. However, this query only shows the I/O statistics for the database instance. In general, optimal preferred read extended cluster configurations balance performance with disk group availability.

See Also:

Oracle Database Reference for details about the `V$ASM*` dynamic performance views

Performance and Scalability Considerations for Disk Groups

This section discusses the following considerations for evaluating disk group performance:

- [Determining the Number of Disk Groups](#)
- [Performance Characteristics When Grouping Disks](#)
- [Oracle ASM Storage Limits](#)

Determining the Number of Disk Groups

Use the following criteria to determine the number of disk groups to create:

- Disks in a given disk group should have similar size and performance characteristics. If you have several different types of disks in terms of size and performance, then create several disk groups that contain similar characteristics.
- Create separate disk groups for your database files and fast recovery area for backup files. This configuration allows fast recovery should a disk group failure occur.

For information about creating disk groups for a new installation, refer to [“Creating Disk Groups for a New Oracle Installation”](#).

Performance Characteristics When Grouping Disks

Oracle ASM load balances the file activity by uniformly distributing file extents across all of the disks in a disk group. For this technique to be effective it is important that disks in a disk group be of similar performance characteristics. For example, the newest and fastest disks might reside in a disk group reserved for the database work area, and slower drives could reside in a disk group reserved for the fast recovery area.

There might be situations where it is acceptable to temporarily have disks of different sizes and performance characteristics coexist in a disk group. This would be the case when migrating from an old set of disks to a new set of disks. The new disks would be added and the old disks dropped. As the old disks are dropped, their storage is migrated to the new disks while the disk group is online.

Oracle ASM Storage Limits

Oracle ASM provides near unlimited capacity for future growth, but does have some storage limits. Oracle ASM has the following limits on the number of disk groups, disks, and files:

- 511 disk groups in a storage system for Oracle Database 12c Release 1 or later
- 10,000 Oracle ASM disks in a storage system
- 1 million files for each disk group

Without any Oracle Exadata Storage, Oracle ASM has the following storage limits if the `COMPATIBLE . ASM` or `COMPATIBLE . RDBMS` disk group attribute is set to less than 12.1:

- 2 terabytes (TB) maximum storage for each Oracle ASM disk
- 20 petabytes (PB) maximum for the storage system

Without any Oracle Exadata Storage, Oracle ASM has the following storage limits if the `COMPATIBLE . ASM` and `COMPATIBLE . RDBMS` disk group attributes are set to 12.1 or greater:

- 4 PB maximum storage for each Oracle ASM disk with the allocation unit (AU) size equal to 1 MB
- 8 PB maximum storage for each Oracle ASM disk with the AU size equal to 2 MB
- 16 PB maximum storage for each Oracle ASM disk with the AU size equal to 4 MB
- 32 PB maximum storage for each Oracle ASM disk with the AU size equal to 8 MB
- 320 exabytes (EB) maximum for the storage system

With all Oracle Exadata Storage, Oracle ASM has the following storage limits:

- 4 PB maximum storage for each Oracle ASM disk with the AU size equal to 1 MB
- 8 PB maximum storage for each Oracle ASM disk with the AU size equal to 2 MB
- 16 PB maximum storage for each Oracle ASM disk with the AU size equal to 4 MB
- 32 PB maximum storage for each Oracle ASM disk with the AU size equal to 8 MB
- 320 EB maximum for the storage system

The maximum size limit of a disk group equals the maximum disk size multiplied by the maximum number of disks in a disk group (10,000).

The maximum number of disks across all disk groups is 10,000. The 10,000 disks can be in one disk group or distributed across a maximum of 511 disk groups. This is a limitation on the number of Oracle ASM disks, not necessarily the number of spindles. A storage array could group multiple spindles into a LUN that is used as a single Oracle ASM disk.

File size limits are dependent on the value of the disk group compatibility attributes. Oracle ASM supports file sizes greater than 128 TB in any redundancy mode when the `COMPATIBLE.RDBMS` disk group attribute is set greater than 10.1.

If `COMPATIBLE.RDBMS` is set to 10.1, the file size limits are less. For example, with `COMPATIBLE.RDBMS` equal to 10.1 and the AU size equal to 1 MB, Oracle ASM file size limits are:

- External redundancy: 16 TB
- Normal redundancy: 5.8 TB
- High redundancy: 3.9 TB

Note:

Oracle Database supports data file sizes up to 128 TB depending on the file system. In addition, Oracle Database has a file size limit that is dependent on the `DB_BLOCK_SIZE` initialization parameter.

For information about Oracle ASM disk group compatibility attributes, see [“Disk Group Compatibility”](#). For information about Oracle ASM file size limits, see [Table 5](#).

Disk Group Compatibility

This section describes disk group compatibility under the following topics:

- [Overview of Disk Group Compatibility](#)
- [Disk Group Compatibility Attributes](#)
- [Setting Disk Group Compatibility Attributes](#)
- [Features Enabled By Disk Group Compatibility Attribute Settings](#)
- [Considerations When Setting Disk Group Compatibility in Replicated Environments](#)

Overview of Disk Group Compatibility

Advancing the disk group compatibility settings enables you to use the new Oracle ASM features that are available in a later release. For example, a disk group with the disk group compatibility attributes set to 12.1 can take advantage of Oracle ASM 12c Release 1 (12.1) features. See [Table 3](#) for the features enabled for combinations of compatibility attribute settings.

The disk group compatibility feature also enables environments to interoperate when they use disk groups from both Oracle Database 10g and Oracle Database 11g instances. For example, disk group compatibility settings that are set to Oracle Database 10g Release 2 (10.2) enable an Oracle Database 10g Release 2 (10.2) client to access a disk group created with Oracle ASM 12c Release 1 (12.1).

The disk group attributes that determine compatibility are `COMPATIBLE.ASM`, `COMPATIBLE.RDBMS`, and `COMPATIBLE.ADVM`. The `COMPATIBLE.ASM` and `COMPATIBLE.RDBMS` attribute settings determine the minimum Oracle Database software version numbers that a system can use for Oracle ASM and the database instance types respectively. For example, if the Oracle ASM compatibility setting is 12.1, and RDBMS compatibility is set to 11.2, then the Oracle ASM software version must be at least 12.1, and the Oracle Database client software version must be at least 11.2. The `COMPATIBLE.ADVM` attribute determines whether the Oracle ASM Dynamic Volume Manager feature can create a volume in a disk group.

When you create a disk group, you can specify the disk group compatibility attribute settings in the `CREATE DISKGROUP` SQL statement. The `ALTER DISKGROUP` SQL statement can update the compatible attribute settings for existing disk groups. See [Table 2](#) for examples of valid combinations of compatible attribute settings.

The compatibility attributes are not set to zero releases, such as 11.0 or 12.0 or any value with all zeroes following the first dot.

You can set and update disk group attributes with the `ASMCMD setattr` command. For information about the `ASMCMD setattr` command, see [“setattr”](#).

Note:

- The disk group compatibility settings determine whether your environment can use the latest Oracle ASM features.
 - The disk group compatibility settings can only be advanced; you cannot revert to a lower compatibility setting. See [“Reverting Disk Group Compatibility”](#).
 - The `COMPATIBLE.ASM` attribute must be advanced before advancing other disk group compatibility attributes and its value must be greater than or equal to the value of other disk group compatibility attributes.
-
-

Disk Group Compatibility Attributes

The disk group compatibility attributes specify the disk group compatibility settings for Oracle ASM and database instances. These attributes are described under the following topics:

- [COMPATIBLE.ASM](#)

- [COMPATIBLE.RDBMS](#)
- [COMPATIBLE.ADVM](#)

COMPATIBLE.ASM

The value for the disk group `COMPATIBLE.ASM` attribute determines the minimum software version for an Oracle ASM instance that can use the disk group. This setting also affects the format of the data structures for the Oracle ASM metadata on the disk. The format of other file contents is determined by Oracle ASM Dynamic Volume Manager (Oracle ADVM) and the database instance.

For Oracle ASM 12c, 12.1 is the default setting for the `COMPATIBLE.ASM` attribute when using ASMCA. The default setting is 10.1 when using the `SQL CREATE DISKGROUP` statement and the `ASMCMD mkdgm` command.

COMPATIBLE.RDBMS

The value for the disk group `COMPATIBLE.RDBMS` attribute determines the minimum `COMPATIBLE` database initialization parameter setting for any database instance that is allowed to use the disk group. Before advancing the `COMPATIBLE.RDBMS` attribute, ensure that the values for the `COMPATIBLE` initialization parameter for all of the databases that access the disk group are set to at least the value of the new setting for `COMPATIBLE.RDBMS`.

For example, if the `COMPATIBLE` initialization parameters of the databases are set to either 11.2 or 12.1, then `COMPATIBLE.RDBMS` can be set to any value between 10.1 and 11.2 inclusively.

For Oracle ASM 12c, 10.1 is the default setting for the `COMPATIBLE.RDBMS` attribute when using the `SQL CREATE DISKGROUP` statement, the `ASMCMD mkdgm` command, and ASMCA.

Note:

The database initialization parameter `COMPATIBLE` enables you to use a new release of Oracle Database, while at the same time guaranteeing backward compatibility with an earlier release. See *Oracle Database Reference* for more information about the `COMPATIBLE` initialization parameter.

COMPATIBLE.ADVM

The value for the disk group `COMPATIBLE.ADVM` attribute determines whether the disk group can contain Oracle ADVM volumes. The value must be set to 11.2 or higher. Before setting this attribute, the `COMPATIBLE.ASM` value must be 11.2 or higher. Also, the Oracle ADVM volume drivers must be loaded in the supported environment.

By default, the value of the `COMPATIBLE.ADVM` attribute is empty until set.

For more information about Oracle ADVM, see “[Overview of Oracle ASM Dynamic Volume Manager](#)”.

Setting Disk Group Compatibility Attributes

This section discusses the settings of the disk group compatibility attributes and how to set the attribute values with the `CREATE DISKGROUP` or `ALTER DISKGROUP` SQL statement.

This section contains these topics:

- [Valid Combinations of Compatibility Attribute Settings](#)
- [Using CREATE DISKGROUP with Compatibility Attributes](#)
- [Using ALTER DISKGROUP with Compatibility Attributes](#)
- [Viewing Compatibility Attribute Settings](#)
- [Reverting Disk Group Compatibility](#)

You can also set the disk group compatibility settings with Oracle ASM command-line utility (ASMCMD) and Oracle ASM Configuration Assistant (ASMCA). Refer to [Managing Oracle ASM With ASMCA](#) and [Managing Oracle ASM with ASMCMD](#).

Note:

Advancing the values for disk group compatibility attributes is an irreversible operation. See [“Reverting Disk Group Compatibility”](#).

See Also:

Oracle Database SQL Language Reference for more information about the disk group compatibility SQL statements

Valid Combinations of Compatibility Attribute Settings

When setting the values for the disk group attributes, specify at least the major and minor versions of a valid Oracle Database release number. For example, you can specify compatibility as '11.2' or '12.1'; Oracle assumes that any missing version number digits are zeros.

[Table 2](#) shows some valid combinations of the disk group compatibility attributes and the valid Oracle ASM and database instance versions for each combination.

Table 2 Examples of disk group compatibility attribute settings

COMPATIBLE.ASM	COMPATIBLE.RDBMS	COMPATIBLE.ADV	Oracle ASM Instance Version	COMPATIBLE Setting for RDBMS Instance
10.1	10.1	n/a	>= 10.1	>= 10.1
11.1	10.1	n/a	>= 11.1	>= 10.1
11.2	11.2	11.2	>= 11.2	>= 11.2
12.1	12.1	12.1	>= 12.1	>= 12.1

These are some possible combinations of Oracle ASM and database releases:

- The database release is Oracle Database 11g Release 2 (11.2) (database initialization parameter `COMPATIBLE` is set to 11.2) and the Oracle ASM release is Oracle ASM 11g Release 2 (11.2). The `COMPATIBLE.ASM` and `COMPATIBLE.RDBMS` disk group attributes are set to 10.2 for a disk group.

The Oracle ASM disk group functionality remains at Oracle Database 10g Release 2 (10.2).

- The database release is Oracle Database 10g Release 1 (10.1) and the Oracle ASM release is 11.2. COMPATIBLE.ASM is set to 11.2 and COMPATIBLE.RDBMS is set to 10.1 for a disk group.

The disk group features enabled for this combination of attribute settings are shown in [Table 3](#).

- The database release is Oracle Database 12c Release 1 (12.1) (database initialization parameter COMPATIBLE is set to 12.1) and the Oracle ASM release is Oracle ASM 12c Release 1 (12.1). All the disk group compatibility attributes are set to 12.1 for a disk group.

The disk group features enabled for this combination of attribute settings are shown in [Table 3](#).

Using CREATE DISKGROUP with Compatibility Attributes

You can specify the compatibility settings for a disk group with the CREATE DISKGROUP statement when creating the disk group.

The following example creates a normal redundancy disk group data1 with the Oracle ASM compatibility set to 12.1 and the RDBMS compatibility set to the default (the COMPATIBLE.RDBMS default is less than or equal to 12.1):

```
CREATE DISKGROUP data1 DISK '/dev/sd*'
  ATTRIBUTE 'compatible.asm' = '12.1';
```

The following example creates a normal redundancy disk group data2 with the ASM, RDBMS, and ADVM compatibility set to 12.1:

```
CREATE DISKGROUP data2 DISK '/dev/sd*'
  ATTRIBUTE 'compatible.asm' = '12.1', 'compatible.rdbms' = '12.1',
  'compatible.advm' = '12.1';
```

Using ALTER DISKGROUP with Compatibility Attributes

After a disk group has been created, you can use the ALTER DISKGROUP SQL statement to change the compatibility attributes. The ALTER DISKGROUP SQL statement ensures that Oracle can advance the compatibility of the specified disk group before committing the change.

All of the affected databases and file systems should be online when running ALTER DISKGROUP to ensure that advancing compatibility does not reduce the database and file system access. When advancing disk group compatibility, you must advance the COMPATIBLE.ASM attribute before the COMPATIBLE.RDBMS or COMPATIBLE.ADVM attribute to ensure a valid combination of compatible attribute settings as shown in [Table 2](#). You can advance only one compatibility attribute in a single ALTER DISKGROUP statement.

The following example advances the Oracle ASM compatibility for disk group data3 to 12.1. An Oracle ASM instance must be at Oracle ASM 12c Release 1 (12.1) or higher to access the data3 disk group.

```
ALTER DISKGROUP data3 SET ATTRIBUTE 'compatible.asm' = '12.1';
```

The following example advances the COMPATIBLE.RDBMS and COMPATIBLE.ADVM compatibility attributes of the disk group data3 to 12.1. This example assumes that the value of COMPATIBLE.ASM is set to 12.1.

```
ALTER DISKGROUP data3 SET ATTRIBUTE 'compatible.rdbms' = '12.1',
ALTER DISKGROUP data3 SET ATTRIBUTE 'compatible.advm' = '12.1';
```

Viewing Compatibility Attribute Settings

You can view the disk group compatibility settings in the `V$ASM_ATTRIBUTE` view. However, the `V$ASM_ATTRIBUTE` view does not display any rows when the `COMPATIBLE.ASM` value is set to 10.1. Instead you can determine the values for the `COMPATIBLE.ASM` and `COMPATIBLE.RDBMS` disk group compatibility attributes with the `COMPATIBILITY` and `DATABASE_COMPATIBILITY` columns of the `V$ASM_DISKGROUP` view.

See [Example 1](#) for an example querying the `V$ASM_ATTRIBUTE` view.

You can also display the disk group compatibility attributes with the `ASMCMD` command `lsattr`. For information about `lsattr`, see ["lsattr"](#).

See Also:

- *Oracle Database SQL Language Reference* for information about disk group attributes
 - *Oracle Database Reference* for details on the `V$ASM_DISKGROUP` and `V$ASM_ATTRIBUTE` dynamic performance views
-
-

Reverting Disk Group Compatibility

Advancing the values for disk group compatibility attributes is an irreversible operation. If you advance the disk group compatibility settings, you cannot change the values back to the previous settings. To revert to the previous values, you must create a new disk group with the old compatibility attribute settings and then restore the database files that were in the disk group to the new disk group.

When you revert to a new disk group with the old compatibility attribute settings, the latest Oracle ASM features might not be available. For example, if you revert the disk group compatibility to a pre-11.2 value, Oracle ACFS functionality is not available.

For example, you could perform the following procedure to revert a disk group to previous compatibility settings:

1. If the Oracle ASM SPFILE is in the disk group, move this SPFILE out of the disk group:
 - a. Connect with SQL*Plus to the Oracle ASM instance.
 - b. Create a PFILE in the file system.

For example:

```
SQL> CREATE PFILE '$ORACLE_HOME/dbs/asmspfile.ora' FROM SPFILE;
```

2. If the OCR and voting files are in the disk group, move them out of this disk group.

See Also:

The *Oracle Clusterware Administration and Deployment Guide* for information about administering OCR and voting files

3. Back up any files that must be saved.
 - a. Back up the database files.
 - b. If an Oracle ACFS file system is mounted on an Oracle ADVM volume on the disk group, the operating system files in the file system must be backed up or copied to a location outside the file system mount point.
4. Create a new disk group using SQL `CREATE DISKGROUP` specifying the previous values for the disk group attribute settings.

For information about creating a disk group, see [“Using the CREATE DISKGROUP SQL Statement”](#).

5. Move or restore the database files into the newly created disk group using either the `ALTER DATABASE MOVE DATAFILE` SQL statement or Recovery Manager (RMAN).

For information about moving data files between disk groups, refer to [“Moving Data Files Between Disk Groups With ALTER DATABASE”](#).

For information about moving database files with RMAN, refer to [“Moving Data Files Between Oracle ASM Disk Groups Using RMAN”](#).

See Also:

Oracle Database Administrator's Guide for information about using the `ALTER DATABASE MOVE DATAFILE` SQL statement to move data files between Oracle ASM disk groups.

6. Drop the disk group with the advanced disk group compatibility settings using SQL `DROP DISKGROUP INCLUDING CONTENTS` to remove the disk group and its contents.

This SQL statement also removes any Oracle ACFS file system and its contents.

For information about dropping a disk group, see [“Dropping Disk Groups”](#).

Features Enabled By Disk Group Compatibility Attribute Settings

[Table 3](#) describes the Oracle ASM features enabled by valid combinations of the disk group compatibility attribute settings.

Table 3 Oracle ASM features enabled by disk group compatibility attribute settings

Disk Group Features Enabled	COMPATIBLE.ASM	COMPATIBLE.RDBMS	COMPATIBLE.ADVM
Support for larger AU sizes (32 or 64 MB)	>= 11.1	>= 11.1	n/a
Attributes are displayed in the <code>V \$ASM_ATTRIBUTE</code> view	>= 11.1	n/a	n/a
Fast mirror resync	>= 11.1	>= 11.1	n/a
Variable size extents	>= 11.1	>= 11.1	n/a
Exadata storage	>= 11.1.0.7	>= 11.1.0.7	n/a
Intelligent Data Placement	>= 11.2	>= 11.2	n/a
OCR and voting files in a disk group	>= 11.2	n/a	n/a

Disk Group Features Enabled	COMPATIBLE.ASM	COMPATIBLE.RDBMS	COMPATIBLE.ADV
Sector size set to nondefault value	>= 11.2	>= 11.2	n/a
Oracle ASM SPFILE in a disk group	>= 11.2	n/a	n/a
Oracle ASM File Access Control	>= 11.2	>= 11.2	n/a
ASM_POWER_LIMIT value up to 1024	>= 11.2.0.2	n/a	n/a
Content type of a disk group	>= 11.2.0.3	n/a	n/a
Replication status of a disk group	>= 12.1	n/a	n/a
Managing a shared password file in a disk group	>= 12.1	n/a	n/a
Greater than 2 TB Oracle ASM disks without Oracle Exadata storage	>= 12.1	>= 12.1	n/a

[Table 4](#) describe the Oracle ACFS features enabled by valid combinations of the disk group compatibility attribute settings.

Table 4 Oracle ACFS features enabled by disk group compatibility attribute settings

Disk Group Features Enabled	COMPATIBLE.ASM	COMPATIBLE.RDBMS	COMPATIBLE.ADV
Volumes in disk groups	>= 11.2	n/a	>= 11.2
Encryption, replication, security, tagging (Linux systems)	>= 11.2.0.2	n/a	>= 11.2.0.2
Read-only snapshots	>= 11.2.0.2	n/a	>= 11.2.0.2
Encryption, replication, security, tagging (Windows systems)	>= 11.2.0.3	n/a	>= 11.2.0.3
Read-write snapshots	>= 11.2.0.3	n/a	>= 11.2.0.3
Unlimited file system expansion	>= 11.2.0.4	n/a	>= 11.2.0.4
Performance and scalability improvements in <code>ls</code> and <code>find</code>	>= 11.2.0.4	n/a	>= 11.2.0.4
Storing database data files and redo logs in Oracle ACFS file systems (on Windows the software must be 12.1.0.2 or higher and COMPATIBLE.ADV must be set to 12.1.0.2)	>= 12.1	n/a	>= 12.1
Encryption, replication, security, tagging (Solaris systems)	>= 12.1	n/a	>= 12.1
Replication and tagging (AIX systems)	>= 12.1	n/a	>= 12.1
Creation from an existing snapshot and conversion of a snapshot	>= 12.1	n/a	>= 12.1
Support for 1023 snapshots	>= 12.1	n/a	>= 12.1.0.2
Accelerator volume for Oracle ACFS file system	>= 12.1	n/a	>= 12.1.0.2

The following list applies to [Table 3](#) and [Table 4](#).

- If encryption is configured for the first time on Oracle ASM 11g Release 2 (11.2.0.3) on Linux or if encryption parameters must be changed or a new volume encryption key must be created following a software upgrade to Oracle ASM 11g Release 2

(11.2.0.3) on Linux, then the disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.3 or higher.

- All database files for Oracle Database can be stored in Oracle ACFS starting with Oracle Database 11g Release 2 (11.2.0.4), except for data files and redo logs in an Oracle Restart configuration. Using replication or encryption with database files on Oracle ACFS is not supported. For additional information, including any limitations or restrictions about storing data files in an Oracle ACFS file system, refer to “[Overview of Oracle ACFS](#)”.
- Oracle ASM and Oracle ACFS features not explicitly listed in [Table 3](#) and [Table 4](#) do not require advancing the disk group compatibility attribute settings.
- Oracle ASM and Oracle ACFS features explicitly identified by an operating system in [Table 3](#) and [Table 4](#) are available on that operating system starting with the associated disk group attribute settings.
- The value of `COMPATIBLE.ASM` must always be greater than or equal to the value of `COMPATIBLE.RDBMS` and `COMPATIBLE.ADVM`.
- A value of not applicable (n/a) means that the setting of the attribute has no effect on the feature.
- For information about the rebalancing process and the `ASM_POWER_LIMIT` initialization parameter, refer to “[ASM_POWER_LIMIT](#)”.

Considerations When Setting Disk Group Compatibility in Replicated Environments

If you advance disk group compatibility, then you could enable the creation of files that are too large to be managed by a previous release of Oracle Database. You must be aware of the file size limits because replicated sites cannot continue using the software from a previous release to manage these large files. The disk group compatibility settings should be the same for all replicated environments.

[Table 5](#) shows the maximum Oracle ASM file sizes supported for `COMPATIBLE.RDBMS` settings when the `AU_SIZE` attribute is set to one megabyte for a disk group.

Table 5 Maximum Oracle ASM file sizes for disk groups with `AU_SIZE` equal to 1 MB

Redundancy	<code>COMPATIBLE.RDBMS = 10.1</code>	<code>COMPATIBLE.RDBMS >= 11.1</code>
External	16 TB	140 PB
Normal	5.8 TB	23 PB
High	3.9 TB	15 PB

[Table 5](#) shows that Oracle Database 10g can only support a file size of up to 16 TB for external redundancy. If you advance the `COMPATIBLE.RDBMS` attribute to 11.1 or greater, then a file can grow beyond 16 TB. However, the larger size causes the file to be unusable in a replicated and disaster recovery site if the disaster recovery site has a disk group `COMPATIBLE.RDBMS` setting that is incompatible with the larger size.

For information about Oracle ASM storage sizes, see “[Oracle ASM Storage Limits](#)”.

See Also:

- *Oracle Database Upgrade Guide* for information about database compatibility
 - *Oracle Database Administrator's Guide* for information about the COMPATIBLE initialization parameter and irreversible compatibility
 - *Oracle Database Reference* for information about the COMPATIBLE initialization parameter
-

Managing Oracle ASM File Access Control for Disk Groups

Oracle ASM File Access Control provides optional protection for the content of Oracle ASM disk groups from accidental access by unauthorized Oracle ASM clients, such as an unauthorized database.

To set up Oracle ASM File Access Control, you must designate separate operating system groups as described in [“Using Separate Operating System Groups for Oracle ASM Users”](#). Oracle ASM File Access Control is available for Linux and UNIX computers only.

You can manage Oracle ASM file access control with ASMCMD commands and SQL statements.

This section contains these topics:

- [About Oracle ASM File Access Control](#)
- [Setting Disk Group Attributes for Oracle ASM File Access Control](#)
- [Using SQL Statements to Manage Oracle ASM File Access Control](#)

For information about managing Oracle ASM File Access Control with ASMCMD commands, see [“ASMCMD File Access Control Commands”](#).

For information about views that provide details about Oracle ASM file access control, see [“Viewing Oracle ASM File Access Control Information”](#).

For information about controlling accessing to Oracle ASM instances, see [“Authentication for Accessing Oracle ASM Instances”](#).

About Oracle ASM File Access Control

Oracle ASM File Access Control restricts the access of files to specific Oracle ASM clients that connect as SYSDBA. An Oracle ASM client is typically a database, which is identified as the user that owns the database instance home. Oracle ASM File Access Control uses this user name to identify a database. Oracle ASM File Access Control restricts access based on the operating system effective user identification number of a database owner. For example, in [Table 2](#) the databases are identified as `oracle1` and `oracle2`.

Oracle ASM uses file access control to determine the additional privileges that are given to a database that has been authenticated AS SYSDBA on the Oracle ASM instance. These additional privileges include the ability to modify and delete certain files, aliases, and user groups.

You can set up user groups to specify the list of databases that share the same access permissions to Oracle ASM files. User groups are lists of databases and any database

that authenticates AS SYSDBA can create a user group. However, only the creator of a group can delete it or modify its membership list.

Each Oracle ASM file has three categories of privileges: owner, group, and other. Each category can have no permission, read-only permission, or read-write permission.

The file owner is usually the creator of the file and can assign permissions for the file in any of the owner, group, or other categories. The owner can also change the group associated with the file.

When you create a file, a group is not automatically associated with the file. You must use the `asmcmd chgrp` command to set the group manually because Oracle ASM File Access Control does not have the concept of the primary group of a user.

When administering Oracle ASM File Access Control, Oracle recommends that you connect as SYSDBA to the database instance that is the owner, or planned owner, of the files in the disk group.

To set up Oracle ASM File Access Control for files in a disk group, perform the following steps:

1. Alter a new or existing disk group to set the Oracle ASM File Access Control disk group attributes.

For a newly-created disk group, you should set the disk group attributes before creating any files in the disk group.

See [“Setting Disk Group Attributes for Oracle ASM File Access Control”](#).

2. For files that exist in a disk group before setting the Oracle ASM File Access Control disk group attributes, you must explicitly set the permissions and ownership on those existing files.

Ensure that the user exists before setting ownership or permissions on a file. The file must be closed before setting the ownership or permissions.

See `ALTER DISKGROUP SET PERMISSION` and `ALTER DISKGROUP SET OWNERSHIP` in [“Using SQL Statements to Manage Oracle ASM File Access Control”](#).

3. Optionally, you can create user groups that are groups of database users that share the same access permissions to Oracle ASM files.

See `ALTER DISKGROUP ADD USERGROUP` in [“Using SQL Statements to Manage Oracle ASM File Access Control”](#).

Setting Disk Group Attributes for Oracle ASM File Access Control

To manage Oracle ASM File Access Control for a disk group, you must set the `ACCESS_CONTROL.ENABLED` and `ACCESS_CONTROL.UMASK` disk group attributes. You can set the attributes by altering the disk group with the `ALTER DISKGROUP SQL` statement or you can set the attributes with the `ASMCMD setattr` command. For information about the `ASMCMD setattr` command, see [“setattr”](#).

When you set up file access control on an existing disk group, the files previously created remain accessible by everyone, unless you run the `ALTER DISKGROUP SET PERMISSION SQL` statement or the `ASMCMD chmod` command to restrict the permissions. For information about the `ASMCMD chmod` command, see [“chmod”](#).

The `COMPATIBLE.ASM` and `COMPATIBLE.RDBMS` disk group attributes must be set to 11.2 or higher to enable Oracle ASM File Access Control. For information about disk group compatibility attributes, see [“Disk Group Compatibility”](#).

The disk group attributes that control Oracle ASM File Access Control are the following:

- `ACCESS_CONTROL.ENABLED`

This attribute determines whether Oracle ASM File Access Control is enabled for a disk group.

The value can be `true` or `false`. The default is `false`.

If the attribute is set to `true`, accessing Oracle ASM files is subject to access control. If `false`, any user can access every file in the disk group. All other operations behave independently of this attribute.

- `ACCESS_CONTROL.UMASK`

This attribute determines which permissions are masked out on the creation of an Oracle ASM file for the user that owns the file, users in the same user group, and others not in the user group. This attribute applies to all files on a disk group.

The values can be combinations of three digits {0|2|6} {0|2|6} {0|2|6}. The default is 066.

Setting to 0 masks out nothing. Setting to 2 masks out write permission. Setting to 6 masks out both read and write permissions.

Before setting the `ACCESS_CONTROL.UMASK` disk group attribute, you must set the `ACCESS_CONTROL.ENABLED` attribute to `true` to enable Oracle ASM File Access Control.

[Example 11](#) shows how to enable Oracle ASM File Access Control for a disk group using SQL*Plus. In this example, the `umask` permissions setting is 026 which enables read-write access for the owner (masks out nothing with 0), read access for users in the group (masks out write permission with 2), and no access to others (masks out all access with 6) not in the group.

Example 11 Setting up Oracle ASM File Access Control

```
ALTER DISKGROUP data1 SET ATTRIBUTE 'access_control.enabled' = 'true';
ALTER DISKGROUP data1 SET ATTRIBUTE 'access_control.umask' = '026';
```

Using SQL Statements to Manage Oracle ASM File Access Control

You can use the `ALTER DISKGROUP` SQL statement to manage file access control for Oracle ASM disk groups. These SQL statements are available for both database and Oracle ASM instances.

When administering users with SQL*Plus, the users must be existing operating system users and their user names must have corresponding operating system user IDs. However, only users in the same cluster as the Oracle ASM instance can be validated.

Note:

When modifying ownership of files, the previous owner of a file cannot be dropped while the file is still open even after the ownership of the file has changed.

The SQL statements that support disk group access control are:

- `ALTER DISKGROUP ADD USERGROUP WITH MEMBER`

Adds an Oracle ASM user group to a disk group. The user group name is limited to a maximum of 30 characters. The operating system users of the databases identified in the MEMBER clause must be in the disk group, as shown by V\$ASM_USER, or the command returns an error. Any users authenticated as SYSASM or SYSDBA can create new user groups. For example:

```
SQL> SELECT group_number, os_name FROM V$ASM_USER;
```

```
GROUP_NUMBER OS_NAME
-----
              1 oracle1
              1 oracle2
...

```

```
SQL> ALTER DISKGROUP data ADD USERGROUP 'test_grp1'
      WITH MEMBER 'oracle1','oracle2';
```

- ALTER DISKGROUP DROP USERGROUP

Drops an Oracle ASM user group from a disk group. Dropping a group might leave some files without a valid group. For those files to have a valid group, you must manually update the group associated with those files to a valid group.

```
SQL> ALTER DISKGROUP data DROP USERGROUP 'test_grp1';
```

- ALTER DISKGROUP MODIFY USERGROUP ADD MEMBER

Adds users to the specified user group. The users must be in the disk group, as shown by V\$ASM_USER, or the command returns an error. Only the creator of the group or the Oracle ASM administrator can modify group membership.

```
SQL> ALTER DISKGROUP data MODIFY USERGROUP 'test_grp2' ADD MEMBER 'oracle2';
```

- ALTER DISKGROUP MODIFY USERGROUP DROP MEMBER

Removes users from the specified user group. If a member is not in the user group, then an error is returned. Only the creator of the group or the Oracle ASM administrator can modify group membership.

```
SQL> ALTER DISKGROUP data MODIFY USERGROUP 'test_grp2' DROP MEMBER 'oracle2';
```

- ALTER DISKGROUP ADD USER

Adds operating system (OS) users to an Oracle ASM disk group, so that these users can have access privileges on the disk group. If a user exists in the disk group, as shown by V\$ASM_USER, then the command records an error and continues to add other users, if any.

The operating system user of a running database instance is automatically added to a disk group when the database instance accesses that disk group and creates files. However, for a database instance to read files in a disk group without creating any files, then you must use the ADD USER clause to add the operating system user associated with that database to the disk group. Also, you can use this clause to add the operating system user associated with a database to an existing disk group immediately after setting the Oracle ASM File Access Control disk group attributes and before creating new files.

```
SQL> ALTER DISKGROUP DATA ADD USER 'oracle1';
```

- ALTER DISKGROUP DROP USER

Drops operating system users from an Oracle ASM disk group. If a user is not in the disk group, then this command records an error and continues to drop other users, if any.

If the user owns any files on the same Oracle ASM disk group, then this command fails with an error, unless the `CASCADE` keyword is specified. If the latter case, then the user is deleted, along with all the files that the user owns.

If any files owned by the user are currently open, then the `DROP USER` command fails, and no files are deleted.

```
SQL> ALTER DISKGROUP DATA DROP USER 'oracle1';
```

- **ALTER DISKGROUP REPLACE USER**

Replaces one operating system user with another in an Oracle ASM disk group. The replacement user must not be a user currently in the disk group user list.

If the command succeeds, all files that were previously owned by current user are now owned by the replacement user. The current user is automatically removed from the user list of the disk group. Adding the current user back to the disk group is possible, but this user does not own any files.

When changing the owner of an open file, the new owner cannot be dropped with the owner's files until all instances within a cluster are restarted.

Only an Oracle ASM administrator can run this command.

```
SQL> ALTER DISKGROUP disk_group REPLACE USER oracle1 WITH oracle2;
```

- **ALTER DISKGROUP SET PERMISSION**

Modifies permissions of an Oracle ASM file. Setting read only permission to a file that has read write permission revokes the write permission. Only the file owner or the Oracle ASM administrator can change the permissions of a file.

```
SQL> ALTER DISKGROUP data SET PERMISSION OWNER=read write, GROUP=read only,
      OTHER=none FOR FILE '+data/controlfile.f';
```

- **ALTER DISKGROUP SET OWNERSHIP**

Changes the owner or group of a file to the specified user or user group name, respectively. If the specified user or user group name does not exist, this command fails with an error. Only the owner of the file or the Oracle ASM administrator can run this command, and only the Oracle ASM administrator can change the owner. Also, the user group name must exist, and the owner of the file must be a member of that group.

```
SQL> ALTER DISKGROUP data SET OWNERSHIP OWNER='oracle1', GROUP='test_grpl'
      FOR FILE '+data/controlfile.f';
```

See Also:

The `ALTER DISKGROUP` SQL statement in the *Oracle Database SQL Language Reference*

Maintaining Disk Groups

This section discusses maintenance operations performed on disk groups.

This section contains the following topics:

- [Mounting and Dismounting Disk Groups](#)
- [Mounting Disk Groups Using the FORCE Option](#)

- [Checking the Internal Consistency of Disk Group Metadata](#)
- [Dropping Disk Groups](#)
- [Renaming Disks Groups](#)

Mounting and Dismounting Disk Groups

Disk groups that are specified in the `ASM_DISKGROUPS` initialization parameter are mounted automatically at Oracle ASM instance startup. This process makes the disk groups available to all database instances running on the same node as Oracle ASM. The disk groups are dismounted at Oracle ASM instance shutdown. Oracle ASM also automatically mounts a disk group when you initially create it, and dismounts a disk group if you drop it.

When a disk group is mounted, a disk group number is chosen. This number may change across disk group mounts. A disk group number is not recorded in any persistent structure, but the current value can be viewed in the `GROUP_NUMBER` column of the `V$ASM` views.

When you want to mount or dismount disk groups manually, use the `ALTER DISKGROUP . . . MOUNT` or `ALTER DISKGROUP . . . DISMOUNT` statement. You can mount or dismount disk groups by name, or specify `ALL`. You can also specify the optional `FORCE` option. For information about using the `FORCE` option, refer to [“Mounting Disk Groups Using the FORCE Option”](#).

If you try to dismount a disk group that contains open files, the statement fails, unless you also specify the `FORCE` clause.

In a clustered Oracle ASM environment in `RESTRICTED` mode, a disk group is mounted in single-instance exclusive mode. No other Oracle ASM instance in that cluster can mount that disk group. In this mode the disk group is not usable by any Oracle ASM client. Use this mode to perform a fast rebalance.

The following SQL statement dismounts all disk groups that are currently mounted to the Oracle ASM instance:

```
ALTER DISKGROUP ALL DISMOUNT;
```

The following SQL statement mounts disk group `data1`:

```
ALTER DISKGROUP data1 MOUNT;
```

Mounting Disk Groups Using the FORCE Option

Oracle ASM provides a `MOUNT FORCE` option with `ALTER DISKGROUP` to enable Oracle ASM disk groups to be mounted in normal or high redundancy modes even though some Oracle ASM disks may be unavailable to the disk group at mount time. The default behavior without the `FORCE` option is to fail to mount a disk group that has damaged or missing disks.

The `MOUNT FORCE` option is useful in situations where a disk is temporarily unavailable and you want to mount the disk group with reduced redundancy while you correct the situation that caused the outage.

To successfully mount with the `MOUNT FORCE` option, Oracle ASM must be able to find at least one copy of the extents for all of the files in the disk group. In this case, Oracle ASM can successfully mount the disk group, but with potentially reduced redundancy.

The disks that Oracle ASM cannot access are placed in an offline mode. Oracle ASM then begins timing the period that these disks are in an offline mode. If the disk offline time period exceeds the timer threshold set by `DISK_REPAIR_TIME` disk group attribute, then those disks are permanently dropped from the disk group. You can change the offline timer after a disk is put in an offline state by using the `ALTER DISKGROUP OFFLINE` statement. For more information about setting the `DISK_REPAIR_TIME` disk group attribute, see [“Oracle ASM Fast Mirror Resync”](#).

Note:

An Oracle ASM instance mounts an incomplete disk group differently depending on the specified compatibility. See [“Features Enabled By Disk Group Compatibility Attribute Settings”](#).

In clustered Oracle ASM environments, if an Oracle ASM instance is not the first instance to mount the disk group, then using the `MOUNT FORCE` statement fails. This is because the disks have been accessed by another instance and the disks are not locally accessible.

If all disks are available, then using the `FORCE` option causes the `MOUNT` command to fail. This discourages unnecessary and improper use of the feature.

The following example shows how to use the `FORCE` option to force the mount of the `data1` disk group:

```
SQL> ALTER DISKGROUP data1 MOUNT FORCE;
```

See Also:

The *Oracle Database SQL Language Reference* for additional information about the `ALTER DISKGROUP` statement and the `FORCE` option

Checking the Internal Consistency of Disk Group Metadata

You can check the internal consistency of disk group metadata using the `ALTER DISKGROUP` statement with the `CHECK` keyword. You can use this statement to check specific files in a disk group, specific disks or all disks in a disk group, or specific failure groups within a disk group. The disk group must be mounted to perform these checks.

By default, the `CHECK DISK GROUP` clause verifies all of the metadata directories. Oracle ASM displays summary errors and writes the details about the errors in an alert log. The `CHECK` keyword performs the following operations:

- Verifies the consistency of the disk
- Cross checks all of the file extent maps and allocation tables for consistency
- Checks that the alias metadata directory and file directory are linked correctly
- Verifies that the alias directory tree is linked correctly
- Checks that Oracle ASM metadata directories do not have unreachable allocated blocks

The `REPAIR | NOREPAIR` clause specifies whether Oracle ASM should attempt to repair errors that are found during the check. The default is `NOREPAIR`. Use the `NOREPAIR` clause to receive alerts about inconsistencies and to suppress Oracle ASM from resolving the errors automatically. The following example statement checks for consistency in the metadata for all disks in the `data1` disk group:

```
ALTER DISKGROUP data1 CHECK ALL;
```

See Also:

The *Oracle Database SQL Language Reference* for additional information about the `CHECK` clause syntax

Dropping Disk Groups

The `DROP DISKGROUP` statement enables you to delete an Oracle ASM disk group and optionally, all of its files. You can specify the `INCLUDING CONTENTS` clause if you also want to delete all files that are contained in the disk group. The default is `EXCLUDING CONTENTS`, which provides syntactic consistency and prevents you from dropping the disk group if it has any contents

The Oracle ASM instance must be started and the disk group must be mounted with none of the disk group files open, in order for the `DROP DISKGROUP` statement to succeed. The statement does not return until the disk group has been dropped.

When you drop a disk group, Oracle ASM dismounts the disk group and removes the disk group name from the `ASM_DISKGROUPS` initialization parameter if a server parameter file is being used. If a text initialization parameter file is being used, and the disk group is mentioned in the `ASM_DISKGROUPS` initialization parameter, then you must remove the disk group name from the `ASM_DISKGROUPS` initialization parameter before the next time that you shut down and restart the Oracle ASM instance.

The following statement deletes `data1`:

```
DROP DISKGROUP data1;
```

After ensuring that none of the files contained in `data1` are open, Oracle ASM rewrites the header of each disk in the disk group to remove Oracle ASM formatting information. The statement does not specify `INCLUDING CONTENTS`, so the drop operation fails if the disk group contains any files.

If an Oracle Automatic Storage Management Cluster File System (Oracle ACFS) file system is mounted on a volume contained in the disk group, then the file system must be dismounted. If the file system has been registered, then it must be deregistered. The `INCLUDING CONTENTS` clause must be used to drop this disk group. All data in the file system is destroyed. To view the volumes and mount paths associated with a disk group, you can query the `V$ASM_VOLUME` view. For an example of a query on the `V$ASM_VOLUME` view, see [Example 9](#). For information about deregistering and dismounting Oracle ACFS file systems, see [“Deregistering_ Dismounting_ and Disabling Volumes and Oracle ACFS File Systems”](#).

If you cannot mount a disk group but must drop it, you can use the `FORCE` option of the `DROP DISKGROUP` statement. This command enables you to remove the headers on disks that belong to a disk group that cannot be mounted by any Oracle ASM instances as shown in the following example:

```
SQL> DROP DISKGROUP data1 FORCE;
```

The disk group on which you perform this operation should not be mounted anywhere in the cluster. When you use the `FORCE` option, the Oracle ASM instance does not attempt to verify that a disk group is being used by another Oracle ASM instance in the same storage subsystem.

Note:

Use the `FORCE` option with extreme caution.

You can also drop disks from a disk group with `ASMCA`. Refer to “[Managing Disk Groups with ASMCA](#)”.

Renaming Disk Groups

The `renamedg` tool enables you to change the name of a cloned disk group. The disk group must be dismounted on all nodes in the cluster before running `renamedg` on the disk group.

`renamedg` renames a disk group using a two-step process:

1. Phase one

This phase generates a configuration file to be used in phase two.

2. Phase two

This phase uses the configuration file to perform the renaming of the disk group.

The syntax is:

```
renamedg {-help | help=true}
```

```
renamedg
  [phase={one|two |both}] dgroupname=diskgroup
  newdgroupname=newdiskgroup [config=configfile]
  [asm_diskstring=discoverystring, discoverystring ...]
  [clean={true|false}] [check={true|false}]
  [confirm={true|false}] [verbose={ true|false}]
  [keep_voting_files={true|false}]
```

- `phase={one|two|both}`

Specifies the phase to be run. Allowed values are `one`, `two`, or `both`. This argument is optional. The default is `both`.

Typically you would run both phases. If a problem occurs during the second phase, then you can rerun `phase two` using the generated configuration file.

- `dgroupname=diskgroup`

Specifies the name of the disk group to be renamed.

- `newdgroupname=newdiskgroup`

Specifies the new name for the disk group.

- `config=configfile`

Specifies the path to the configuration file to be generated during phase one or specifies the path to the configuration file to be used during phase two.

This argument is optional. The default configuration file is named `renamedg_config` and is located in the directory in which the command is run. The single quotations may be required on some platforms.

- `asm_diskstring=discoverystring, discoverystring ...`
Specifies the Oracle ASM discovery strings. The `asm_diskstring` value must be specified if the Oracle ASM disks are not in the default location for the platform. The single quotations may be required on some platforms, usually when wildcard characters are specified.
- `clean={true|false}`
Specifies whether to clean errors that are otherwise ignored. The default is `true`.
- `check={true|false}`
Specifies a boolean value that is used in the second phase. If `true`, then the tool prints the list of changes that are to be made to the disks. No writes are issued. It is an optional parameter that defaults to `false`.
- `confirm={true|false}`
Specifies a boolean value that is used in the second phase. If `false`, then the tool prints the changes that are to be made and seeks confirmation before actually making the changes. It is an optional value that defaults to `false`. If `check` is set to `true`, then the value of this parameter is redundant.
- `verbose={true|false}`
Specifies verbose execution when `verbose=true`. The default is `false`.
- `keep_voting_files={true|false}`
Specifies whether voting files are kept in the renamed disk group. The default is `false` which deletes the voting files from the renamed disk group.

Note:

`renamedg` does not update resources, nor does `renamedg` update any file references within the database. Because of this behavior, the original disk group resource is not automatically deleted after the completion of phase two. The status of the old disk group resource can be checked with the Oracle Clusterware Control (CRSCTL) `crsctl stat res -t` command and then manually deleted with the Server Control Utility (SRVCTL) `srvctl remove diskgroup` command.

[Example 12](#) shows several examples of the use of `renamedg`. The first example renames the `fra1` disk group to `fra2` using a disk string to locate the disks and the `verbose` option is enabled. The second example only creates a configuration file during the completion of phase one of the `renamedg` operation. The third example runs phase two of the `renamedg` operation using a configuration file generated from a phase one execution of `renamedg`.

After renaming a disk group, you can rename the disks in the disk group to match the new disk group name. For example:

```
SQL> ALTER DISKGROUP fra2 RENAME DISKS ALL;
```

For information about renaming disks, refer to [“Renaming Disks in Disk Groups”](#).

Example 12 Using renamedg

```
$ renamedg dname=fra1 newdname=fra2 asm_diskstring='/devices/disk*'
    verbose=true

$ renamedg phase=one dname=fra1 newdname=fra2
    asm_diskstring='/devices/disk*' config=/tmp/fra2.conf verbose=true

$ renamedg phase=two dname=fra1 newdname=fra2 config=/tmp/fra2.conf
    verbose=true
```

Administering Oracle ASM Files, Directories, and Templates

This chapter describes how to administer files when you use the Oracle Automatic Storage Management (Oracle ASM) storage option.

This chapter contains the following topics:

- [What Types of Files Does Oracle ASM Support?](#)
- [About Oracle ASM File Names](#)
- [Creating and Referencing Oracle ASM Files in the Database](#)
- [Managing Alias Names for Oracle ASM File Names](#)
- [Managing Disk Group Directories](#)
- [Accessing Oracle ASM Files with the XML DB Virtual Folder](#)
- [Using DBMS_FILE Transfer Utility for Oracle ASM](#)
- [Managing Disk Group Templates](#)

What Types of Files Does Oracle ASM Support?

Oracle ASM supports most file types required by the database. [Table 1](#) lists file types that are supported directly by Oracle ASM and lists the system default template that provides the attributes for file creation. Some file types shown in the table are related to specific products or features, and are not discussed in this book.

Table 1 *File types supported by Oracle ASM*

File Type	Default Templates
Archive log files	ARCHIVELOG
Oracle ASM Persistent initialization parameter file (SPFILE)	ASMPARAMETERFILE
Oracle ASM Persistent initialization parameter file (SPFILE) backup	ASMPARAMETERFILEBACKUP
Audit spill files	AUDIT_SPILLFILES
Automatically generated control file backup	AUTOBACKUP
Auto-login software keystore	AUTOLOGIN_KEY_STORE
Archive log backup piece	BACKUPSET
Data file backup pieces	BACKUPSET

File Type	Default Templates
Data file incremental backup pieces	BACKUPSET
Change tracking file	CHANGETRACKING
Control files	CONTROLFILE
Data file copy	DATAFILE
Data files	DATAFILE
Data Guard configuration file	DATAGUARDCONFIG
Data Pump dumpset	DUMPSET
Flashback logs	FLASHBACK
Flash file	FLASHFILE
Cross-platform transportable data files incremental backup	INCR XTRANSPORT BACKUPSET
Software keystore	KEY_STORE
Oracle Cluster Registry file	OCRFILE
Redo log files	ONLINELOG
Persistent initialization parameter file (SPFILE)	PARAMETERFILE
Temporary files	TEMPFILE
Voting files	VOTINGFILE
Cross-platform transportable data files	XTRANSPORT
Cross-platform transportable data files backup	XTRANSPORT BACKUPSET
Oracle ASM Dynamic Volume Manager volumes	n/a

Oracle ASM cannot directly support some administrative file types on disk groups. These include trace files, audit files, alert logs, export files, tar files, and core files.

Note:

Oracle Automatic Storage Management Cluster File System (Oracle ACFS) and Oracle ASM Dynamic Volume Manager (Oracle ADVM) extend Oracle ASM support to include database and application executables, database data files, database trace files, database alert logs, application reports, BFILES, and configuration files. Other supported files are video, audio, text, images, engineering drawings, and other general-purpose application file data. See [Introducing Oracle ACFS and Oracle ADVM](#).

For a description of the system default templates, refer to “[Managing Disk Group Templates](#)”. For an example of the output of the `V$ASM_TEMPLATE` view, refer to [Example 10](#). For an example of the output of the `ASMCMD lstmpl` command, refer to “[lstmpl](#)”.

About Oracle ASM File Names

Every file created in Oracle ASM is provided a file name generated by Oracle Managed Files, known as a fully qualified file name (or system-generated file name).

The fully qualified file name represents a complete path name in the Oracle ASM file system. An example of a fully qualified file name is:

```
+data/orcl/controlfile/Current.256.541956473
```

You can use the fully qualified file name to reference (read or retrieve) an Oracle ASM file. You can also use other abbreviated file name formats, such as an alias Oracle ASM file name described in “[Alias Oracle ASM File Name Forms](#)”, to reference an Oracle ASM file.

Oracle ASM generates a fully qualified file name upon any request to create a file. A creation request does not or cannot specify a fully qualified file name. Instead, it uses a simpler syntax to specify a file, such as an alias or just a disk group name. Oracle ASM then creates the file, placing it in the correct Oracle ASM path according to file type, and then assigns an appropriate fully qualified file name. If you specify an alias in the creation request, Oracle ASM also creates the alias so that it references the fully qualified file name.

Oracle ASM file creation requests are either single file creation requests or multiple file creation request.

Note:

- You can find the generated name in database views displaying Oracle file names, such as `V$DATAFILE` and `V$LOGFILE`. You can use this name, or an abbreviated form of it, if you later must reference an Oracle ASM file in a SQL statement. As with other Oracle Database file names, Oracle ASM file names are kept in the control file and the RMAN catalog.
- You can use fully qualified and numeric file names in single-file creation if you specify the `REUSE` keyword, as described in “[Using Oracle ASM File Names in SQL Statements](#)”.
- Forward slash (/) and backslash (\) are interchangeable in file names. File names are case insensitive, but case retentive.

This section contains the following topics:

- [Single File Creation Form](#)
- [Multiple File Creation Form](#)
- [Fully Qualified File Name Form](#)
- [Alias Oracle ASM File Name Forms](#)
- [Creating a Tablespace in Oracle ASM: Using a Data File with an Alias Name](#)
- [Alias Oracle ASM File Name with Template Form](#)
- [Incomplete Oracle ASM File Name Form](#)
- [Incomplete Oracle ASM File Name with Template Form](#)

[Table 2](#) specifies the valid usage for each file name form. If the form is used for file creation, the table specifies whether the created file is an Oracle Managed Files (OMF).

Table 2 Valid usage for Oracle ASM file name forms

File Name Form	Reference to File?	Single-file Creation?	Multiple File Creation?	Created as OMF?
Fully qualified file name	Yes	No	No	No
Alias file name	Yes	Yes	No	No
Alias with template file name	No	Yes	No	No
Incomplete file name	No	Yes	Yes	Yes
Incomplete file name with template	No	Yes	Yes	Yes

Single File Creation Form

A single file creation form is used to create a single file, such as a data file or a control file. The form of the Oracle ASM file name in this type is either an alias, such as `+data/orcl/ctl.f`, or an incomplete file name, such as a disk group name preceded by a plus sign (`+data`). You use the alias or disk group name where a file name is called for in a SQL statement, such as `CREATE TABLESPACE`, `CREATE CONTROLFILE`.

Multiple File Creation Form

A multiple file creation form is used multiple times to create Oracle ASM files, such as when assigning a value to the initialization parameter `DB_CREATE_FILE_DEST`. You can also run a `CREATE TABLESPACE` statement (without a file name specification) multiple times. Each time, Oracle ASM creates a different unique data file name.

When using the multiple file creation form, you can use an incomplete file name form, such as a disk group name preceded by a plus sign (`+data`). In this case, you set `DB_CREATE_FILE_DEST` to an incomplete file name (for example, `+data`), and whenever a command is run that must create a database file in `DB_CREATE_FILE_DEST`, the file is created in the designated disk group and assigned a unique fully qualified name. You can use an incomplete file name in other `*_DEST` initialization parameters.

Fully Qualified File Name Form

You can use a fully qualified form for referencing existing Oracle ASM files in Oracle ASM operations, except for disk group creation. This form is the Oracle ASM file name that Oracle ASM automatically generates when an Oracle ASM file is created.

A fully qualified file name has the following form:

```
+diskgroup/dbname/filetype/filetypetag.file.incarnation
```

Where:

- *+diskgroup* is the disk group name preceded by a plus sign.
You can think of the plus sign (+) as the root directory of the Oracle ASM file system, similar to the slash (/) on UNIX or Linux computers.
- *dbname* is the `DB_UNIQUE_NAME` of the database to which the file belongs.
- *filetype* is the Oracle file type and can be one of the file types shown in [Table 3](#).
- *filetypetag* is type-specific information about the file and can be one of the tags shown in [Table 3](#).

- *file.incarnation* is the file/incarnation pair, used to ensure uniqueness.

An example of a fully qualified Oracle ASM file name is:

```
+data/orcl/controlfile/Current.256.541956473
```

Table 3 Oracle file types and Oracle ASM file type tags

Oracle ASM File Type	Description	Oracle ASM File Type Tag	Comments
CONTROLFILE	Control files and backup control files	Current Backup	Archive Backup
DATAFILE	Data files and data file copies	<i>tblspname</i>	Name of the tablespace into which the file is added
ONLINELOG	Online logs	<i>group_loggroup#</i>	
ARCHIVELOG	Archive logs	<i>thread_thread#_seq_sequence#</i>	
TEMPFILE	Tempfiles	<i>tsname</i>	Name of the tablespace into which the file is added
BACKUPSET	Data file and archive log backup pieces; data file incremental backup pieces	<i>spfile?_timestamp</i>	<i>spfile?</i> can take one of two values: <i>s</i> indicates that the backup set includes the <i>spfile</i> ; <i>n</i> indicates that the backup set does not include the <i>spfile</i> . <i>timestamp</i> is the time that the backup is started.
PARAMETERFILE	Persistent parameter files	<i>spfile</i>	Name of the SPFILE
DATAGUARDCONFIG	Data Guard configuration file	<i>db-unique-name</i>	Data Guard uses the value of the DB_UNIQUE_NAME initialization parameter.
FLASHBACK	Flashback logs	<i>log_flashbacklog#</i>	
CHANGETRACKING	Block change tracking data	<i>ctf</i>	Used during incremental backups
DUMPSET	Data Pump dumpset	<i>user_obj#_file#</i>	Dump set files encode the user name, the job number that created the dump set, and the file number as part of the tag.
XTRANSPORT	Data file convert	<i>tblspname</i>	Name of the tablespace where the Oracle ASM metadata is added
AUTOBACKUP	Automatic backup files	<i>spfile?_timestamp</i>	<i>spfile?</i> can take one of two values: <i>s</i> indicates that the backup set includes the <i>spfile</i> ; <i>n</i> indicates that the backup set does not include the <i>spfile</i> . <i>timestamp</i> is the time that the backup is started.
ASMPARAMETERFILE	Oracle ASM persistent parameter files	<i>spfile</i>	Name of the Oracle ASM SPFILE
OCRFILE	Oracle Clusterware Registry files	<i>ocrfile</i>	Name of the OCR files

Alias Oracle ASM File Name Forms

You can use Alias Oracle ASM file names both for referencing existing Oracle ASM files and for creating new Oracle ASM files. Alias names start with the disk group name preceded by a plus sign, after which you specify a name string. Alias file names are implemented using a hierarchical directory structure, with the slash (/) or backslash (\) character separating name components. You can create an alias in any Oracle ASM directory generated by Oracle Managed Files (system-generated) or created by a user. An alias must include the disk group name; you cannot create an alias at the root level (+).

When you create an Oracle ASM file with an alias file name, the file is created with a fully qualified name, and the alias file name is additionally created. You can then access the file with either name.

Alias Oracle ASM file names are distinguished from fully qualified file names or numeric file names because they do not end in a dotted pair of numbers. It is an error to attempt to create an alias that ends in a dotted pair of numbers, such as in the format `USERS.259.685366091`. Examples of Oracle ASM alias file names are:

```
+data/orcl/control_file1  
+fra/recover/second.dbf
```

Oracle Database references database files by their alias file names, but only if you create the database files with aliases. If you create database files without aliases and then add aliases later, the database references the files by their fully qualified file names. The following are examples of how the database uses alias file names:

- Alias file names appear in V\$ views. For example, if you create a tablespace and use an alias file name for the data file, the `V$DATAFILE` view shows the alias file name.
- When a control file points to data files and online redo log files, it can use alias file names.
- The `CONTROL_FILES` initialization parameter can use the alias file names of the control files. Database Configuration Assistant (DBCA) creates control files with alias file names.

Note:

Files created using an alias file name are not considered Oracle Managed Files and might require manual deletion in the future if they are no longer needed.

For more information about alias file names, see [“Managing Alias Names for Oracle ASM File Names”](#).

Creating a Tablespace in Oracle ASM: Using a Data File with an Alias Name

Example 1 creates an undo tablespace with a data file that has an alias name, and with attributes that are set by the user-defined template `my_undo_template`. This example assumes that a directory has been created in disk group `data` to contain the alias name and that the user-defined template exists.

Because an alias is used when creating the data file, the file is not an Oracle Managed Files (OMF) file and the file is not automatically deleted when the tablespace is

dropped. To drop the file manually after the tablespace has been dropped, use the following SQL statement:

```
ALTER DISKGROUP data DROP FILE '+data/orcl/my_undo_ts';
```

Example 1 Creating a tablespace using an alias name

```
CREATE UNDO TABLESPACE myundo
  DATAFILE '+data(my_undo_template)/orcl/my_undo_ts' SIZE 200M;
```

Alias Oracle ASM File Name with Template Form

An alias Oracle ASM file name with template is used only for Oracle ASM file creation operations. It has the following format:

```
+diskgroup(template name)/alias
```

Alias file names with template behave identically to alias file names except that a file created with an alias file name with template receives the attributes specified by the named template. The template must belong to the disk group that the file is being created in. See [Example 1](#).

The creation and maintenance of Oracle ASM templates is discussed in “[Managing Disk Group Templates](#)”.

An example of an alias Oracle ASM file name with template is:

```
+data(mytemplate)/config1
```

Explicitly specifying a template name, as in the previous example, overrides the system default template for the type of file being created.

Note:

Files created using an alias file name with template are not considered Oracle Managed Files and might require manual deletion in the future if they are no longer needed.

Incomplete Oracle ASM File Name Form

Incomplete Oracle ASM file names are used only for file creation operations and are used for both single and multiple file creation. They consist only of the disk group name. Oracle ASM uses a system default template to determine the Oracle ASM file mirroring and striping attributes. The system template that is used is determined by the file type that is being created. For example, if you are creating a data file for a tablespace, then the DATAFILE template is used.

An example of using an incomplete Oracle ASM file name is setting the DB_CREATE_FILE_DEST initialization parameter to:

```
+data
```

With this setting, every time you create a tablespace, a data file is created in the disk group data, and each data file is assigned a different fully qualified name. See “[Creating Oracle ASM Files Using a Default File Location for Disk Group Specification](#)” for more information.

Incomplete Oracle ASM File Name with Template Form

Incomplete Oracle ASM file names with templates are used only for file creation operations and are used for both single and multiple file creation. They consist of the disk group name followed by the template name in parentheses. When you explicitly specify a template in a file name, Oracle ASM uses the specified template instead of the default template for that file type to determine attributes for the file.

An example of using an incomplete Oracle ASM file name with template is setting the `DB_CREATE_FILE_DEST` initialization parameter to:

```
+data(mytemplate)
```

Creating and Referencing Oracle ASM Files in the Database

An Oracle ASM file is an Oracle Managed File unless you created the file using an alias. Any Oracle Managed File is automatically deleted when it is no longer needed.

This section contains the following topics:

- [Creating Oracle ASM Files Using a Default File Location for Disk Group Specification](#)
- [Using Oracle ASM File Names in SQL Statements](#)
- [Moving Data Files Between Disk Groups With ALTER DATABASE](#)
- [Oracle Database File Mapping for Oracle ASM Files](#)

Creating Oracle ASM Files Using a Default File Location for Disk Group Specification

Using the Oracle Managed Files feature for operating system files, you can specify a directory as the default location for the creation of data files, temporary files, redo log files, and control files. Using the Oracle Managed Files feature for Oracle ASM, you can specify a disk group, in the form of an incomplete Oracle ASM file name, as the default location for creation of these files, and additional types of files, including archived log files. As for operating system files, the name of the default disk group is stored in an initialization parameter and is used whenever a file specification (for example, `DATAFILE` clause) is not explicitly specified during file creation.

The following initialization parameters accept the multiple file creation context form of Oracle ASM file names as a destination:

- `DB_CREATE_FILE_DEST`
Specifies the default disk group location in which to create data and temp files.
- `DB_CREATE_ONLINE_LOG_DEST_n`
Specifies the default disk group location in which to create redo log and control files.
- `DB_RECOVERY_FILE_DEST`
Specifies a default disk group for a fast recovery area that contains a copy of the control file and redo log files if this parameter is specified and `DB_CREATE_ONLINE_LOG_DEST_n` and `CONTROL_FILES` are not specified.
- `CONTROL_FILES`

Specifies a disk group in which to create control files.

The following initialization parameters accept the multiple file creation context form of the Oracle ASM file names and Oracle ASM directory names as a destination:

- `LOG_ARCHIVE_DEST_n`
Specifies a default disk group or Oracle ASM directory as destination for archiving redo log files
- `LOG_ARCHIVE_DEST`
Optional parameter to use to specify a default disk group or Oracle ASM directory as destination for archiving redo log files. Use when specifying only one destination.
- `STANDBY_ARCHIVE_DEST`
Relevant only for a standby database. It specifies a default disk group or Oracle ASM directory that is the location of archive logs arriving from a primary database. Not discussed in this book. This parameter has been deprecated. See *Oracle Data Guard Concepts and Administration*.

The following `CREATE TABLESPACE` SQL statement illustrates how an Oracle ASM file, in this case a data file, might be created in a default disk group. This example assumes that the `DB_CREATE_FILE_DEST` initialization parameter has been set to `+data`.

```
SQL> CREATE TABLESPACE mytblspace;
```

Oracle ASM automatically creates and manages the data file for `mytblspace` on Oracle ASM disks in the disk group `data`. File extents are stored using the attributes defined by the default template for a data file.

See Also:

- *Oracle Database Reference* for information about initialization parameters
 - *Oracle Database Administrator's Guide* for information about initialization parameter files
-
-

Using Oracle ASM File Names in SQL Statements

You can specify Oracle ASM file names in the file specification clause of your SQL statements. If you are creating a file for the first time, then use the creation form of an Oracle ASM file name. If the Oracle ASM file exists, then you must use the reference form of the file name, and if you are trying to re-create the file, you must add the `REUSE` keyword so that the space is reused for the new file. This usage might occur when, for example, trying to re-create a control file, as shown in “[Creating Control Files in Oracle ASM](#)”.

If a reference form is used with the `REUSE` keyword and the file does not exist, an error results.

[Example 2](#) is an example of specifying an Oracle ASM file name in a SQL statement. In this case, it is used in the file creation form.

The tablespace `mytblspace` is created and comprises one data file of size 200 MB contained in the disk group `data`. The data file is set to auto-extensible with an unlimited maximum size. You can use an `AUTOEXTEND` clause to override this default.

For more examples of the use of Oracle ASM file name in SQL statements, see [Creating Database Files in Oracle ASM Using SQL*Plus](#).

Example 2 Using an Oracle ASM File name in a SQL statement

```
CREATE TABLESPACE mytblspace DATAFILE '+data' SIZE 200M AUTOEXTEND ON;
```

Moving Data Files Between Disk Groups With ALTER DATABASE

You can use the `ALTER DATABASE MOVE DATAFILE` SQL statement to move data files between disk groups while the database is open and users are accessing the data files.

[Example 3](#) shows how you can move a data file from the `DATA` disk group to the `DATA2` disk group.

See Also:

- *Oracle Database Administrator's Guide* for more information about using the `ALTER DATABASE MOVE DATAFILE` SQL statement to move data files
 - *Oracle Database SQL Language Reference* for information about using the `ALTER DATABASE` SQL statement.
 - ["Moving Data Files Between Oracle ASM Disk Groups Using RMAN"](#) for information about using RMAN to move data files between disk groups
-

Example 3 Moving data files online with ALTER DATABASE MOVE DATAFILE

```
/* Create a new disk group DATA2 using ASMCA, ASMCMD, or SQL */
/* Then create appropriate directories in the DATA2 disk group */

ALTER DISKGROUP data2 ADD DIRECTORY '+DATA2/ORCL';

ALTER DISKGROUP data2 ADD DIRECTORY '+DATA2/ORCL/DATAFILE';

/* Move the EXAMPLE data file in DATA to EXAMPLE_STORAGE in DATA2
ALTER DATABASE MOVE DATAFILE '+DATA/ORCL/DATAFILE/EXAMPLE.266.798707687'
    TO '+DATA2/ORCL/DATAFILE/EXAMPLE_STORAGE';

SELECT SUBSTR(name,1,64) FROM V$DATAFILE;

SUBSTR(NAME,1,64)
-----
+DATA/ORCL/DATAFILE/system.258.798707555
+DATA2/ORCL/DATAFILE/example_storage
+DATA/ORCL/DATAFILE/sysaux.257.798707491
+DATA/ORCL/DATAFILE/undotbs1.260.798707621
+DATA/ORCL/DATAFILE/users.259.798707621
```

Oracle Database File Mapping for Oracle ASM Files

For an understanding of I/O performance, you must have detailed knowledge of the storage hierarchy in which files reside. Oracle Database provides a set of dynamic performance views to show a complete mapping of a file to intermediate layers of logical volumes to actual physical devices. Using these dynamic views, you can locate the exact disk on which any block of a file resides.

Oracle Database communicates with a background process called FMON to manage the mapping information. Oracle provides the PL/SQL `DBMS_STORAGE_MAP` package to invoke mapping operations that populate the mapping views.

Oracle Database file mapping does not require third party libraries when mapping Oracle ASM files. In addition, Oracle Database supports Oracle ASM file mapping on all operating system platforms.

All the example in this section are run on the Oracle Database instance.

For information about file mapping with Oracle ACFS files, refer to [“Oracle ACFS Support for Oracle Database File Mapping Views”](#).

This section contains the following topics:

- [Enabling File Mapping With Oracle ASM Files](#)
- [Using File Mapping Views With Oracle ASM Files](#)
- [Using the `DBMS_STORAGE_MAP` Package With Oracle ASM Files](#)

See Also:

Oracle Database Administrator's Guide for additional information about Oracle Database file mapping

Enabling File Mapping With Oracle ASM Files

To enable file mapping, set the `FILE_MAPPING` initialization parameter to `TRUE`. The database instance does not have to be shut down to set this parameter. You can set the parameter using the following `ALTER SYSTEM` statement:

```
SQL> ALTER SYSTEM SET FILE_MAPPING=TRUE;
```

Run the appropriate `DBMS_STORAGE_MAP` mapping procedure.

- In a cold startup scenario, the Oracle Database has just started and no mapping operation has been invoked yet. You can execute the `DBMS_STORAGE_MAP.MAP_ALL` procedure to build the mapping information for the entire I/O subsystem associated with the database.

For example, the following command builds mapping information and provides for 10000 extents:

```
SQL> EXECUTE DBMS_STORAGE_MAP.MAP_ALL(10000);
```

- In a warm start scenario where the mapping information has already been built, you have the option to invoke the `DBMS_STORAGE_MAP.MAP_SAVE` procedure to save the mapping information in the data dictionary.

This procedure is invoked in `DBMS_STORAGE_MAP.MAP_ALL()` by default. This forces all of the mapping information in the SGA to be flushed to disk. The `DBMS_STORAGE_MAP.MAP_SAVE` procedure is invoked in `DBMS_STORAGE_MAP.MAP_ALL()` by default.

After you restart the database, use `DBMS_STORAGE_MAP.RESTORE()` to restore the mapping information into the SGA. If needed, `DBMS_STORAGE_MAP.MAP_ALL()` can be called to refresh the mapping information.

Using File Mapping Views With Oracle ASM Files

Mapping information generated by DBMS_STORAGE_MAP package is captured in dynamic performance views. These views include V\$MAP_COMP_LIST, V\$MAP_ELEMENT, V\$MAP_EXT_ELEMENT, V\$MAP_FILE, V\$MAP_FILE_EXTENT, V\$MAP_FILE_IO_STACK, V\$MAP_LIBRARY, and V\$MAP_SUBELEMENT.

For example, you can view file mappings with V\$MAP_FILE.

```
SQL> SELECT FILE_MAP_IDX, SUBSTR(FILE_NAME,1,45), FILE_TYPE, FILE_STRUCTURE FROM V$MAP_FILE;
```

FILE_MAP_IDX	SUBSTR(FILE_NAME,1,45)	FILE_TYPE	FILE_STRU
0	+DATA/ORCL/DATAFILE/system.258.841314095	DATAFILE	ASMFILE
1	+DATA/ORCL/DATAFILE/sysaux.257.841314021	DATAFILE	ASMFILE
2	+DATA/ORCL/DATAFILE/undotbs1.260.841314161	DATAFILE	ASMFILE
3	+DATA/ORCL/DATAFILE/example.266.841314219	DATAFILE	ASMFILE
4	+DATA/ORCL/DATAFILE/users.259.841314161	DATAFILE	ASMFILE
5	+DATA/ORCL/ONLINELOG/group_3.264.841314209	LOGFILE	ASMFILE
6	+FRA/ORCL/ONLINELOG/group_3.259.841314211	LOGFILE	ASMFILE
7	+DATA/ORCL/ONLINELOG/group_2.263.841314207	LOGFILE	ASMFILE
8	+FRA/ORCL/ONLINELOG/group_2.258.841314207	LOGFILE	ASMFILE
9	+DATA/ORCL/ONLINELOG/group_1.262.841314203	LOGFILE	ASMFILE
10	+FRA/ORCL/ONLINELOG/group_1.257.841314203	LOGFILE	ASMFILE
11	+DATA/ORCL/TEMPFILE/temp.265.841314217	TEMPFILE	ASMFILE
12	+DATA/ORCL/CONTROLFILE/current.261.841314199	CONTROLFILE	ASMFILE
13	+FRA/ORCL/CONTROLFILE/current.256.841314201	CONTROLFILE	ASMFILE

See Also:

Oracle Database Reference for information about dynamic views

Using the DBMS_STORAGE_MAP Package With Oracle ASM Files

You can use the procedures in the DBMS_STORAGE_MAP PL/SQL package to control mapping operations. For example, you can use the DBMS_STORAGE_MAP.MAP_OBJECT procedure to build mapping information for the database object that is specified by object name, owner, and type. After the DBMS_STORAGE_MAP.MAP_OBJECT procedure is run, then you can create a query to display the mapping information contained in the MAP_OBJECT view.

```
SQL> EXECUTE DBMS_STORAGE_MAP.MAP_OBJECT('EMPLOYEES','HR','TABLE');
```

```
SQL> SELECT io.OBJECT_NAME o_name, io.OBJECT_OWNER o_owner, io.OBJECT_TYPE o_type,
mf.FILE_NAME, me.ELEM_NAME, io.DEPTH,
(SUM(io.CU_SIZE * (io.NUM_CU - DECODE(io.PARITY_PERIOD, 0, 0,
TRUNC(io.NUM_CU / io.PARITY_PERIOD)))) / 2) o_size
FROM MAP_OBJECT io, V$MAP_ELEMENT me, V$MAP_FILE mf
WHERE io.OBJECT_NAME = 'EMPLOYEES'
AND io.OBJECT_OWNER = 'HR'
AND io.OBJECT_TYPE = 'TABLE'
AND me.ELEM_IDX = io.ELEM_IDX
AND mf.FILE_MAP_IDX = io.FILE_MAP_IDX
GROUP BY io.ELEM_IDX, io.FILE_MAP_IDX, me.ELEM_NAME, mf.FILE_NAME, io.DEPTH,
io.OBJECT_NAME, io.OBJECT_OWNER, io.OBJECT_TYPE
ORDER BY io.DEPTH;
```

O_NAME	O_OWNER	O_TYPE	FILE_NAME	ELEM_NAME	DEPTH	O_SIZE
EMPLOYEES	HR	TABLE	+DATA/ORCL/DATAFILE/example.266.841314219	+/devices/diskd2	0	64
EMPLOYEES	HR	TABLE	+DATA/ORCL/DATAFILE/example.266.841314219	+/devices/diske2	0	64

See Also:

Oracle Database PL/SQL Packages and Types Reference for information about the `DBMS_STORAGE_MAP` package

Managing Alias Names for Oracle ASM File Names

Alias names, or aliases, are intended to provide a more user-friendly means of referring to Oracle ASM files, rather than using the system-generated file names.

You can create an alias for a file when you create it in the database, or you can add an alias to an existing file using the `ADD ALIAS` clause of the `ALTER DISKGROUP` statement. You can create an alias in any system-generated or user-created Oracle ASM directory. An alias must include the disk group name; you cannot create an alias at the root level (+).

For more information about creating aliases with `ASMCMD`, refer to “[mkalias](#)”.

This section contains the following sections:

- [Adding an Alias Name for an Oracle ASM File Name](#)
- [Renaming an Alias Name for an Oracle ASM File Name](#)
- [Dropping an Alias Name for an Oracle ASM File Name](#)
- [Dropping Files and Associated Aliases from a Disk Group](#)

Adding an Alias Name for an Oracle ASM File Name

Use the `ADD ALIAS` clause of the `ALTER DISKGROUP` statement to create an alias name for an Oracle ASM file name. The alias name must consist of the full directory path and the alias itself.

[Example 4](#) adds a new alias name for a system-generated file name.

Example 4 Adding an alias name for an Oracle ASM file name

```
ALTER DISKGROUP data ADD ALIAS '+data/orcl/second.dbf'  
FOR '+data/orcl/datafile/mytable.342.123456789';
```

Renaming an Alias Name for an Oracle ASM File Name

Use the `RENAME ALIAS` clause of the `ALTER DISKGROUP` statement to rename an alias for an Oracle ASM file name. The old and the new alias names must consist of the full directory paths of the alias names.

[Example 5](#) renames an alias.

Renaming an alias does not update the database reference to the alias.

Example 5 Renaming an alias name for an Oracle ASM file name

```
ALTER DISKGROUP data RENAME ALIAS '+data/orcl/datafile.dbf'  
TO '+data/payroll/compensation.dbf';
```

Dropping an Alias Name for an Oracle ASM File Name

Use the `DROP ALIAS` clause of the `ALTER DISKGROUP` statement to drop an alias for an Oracle ASM file name. The alias name must consist of the full directory path and the alias itself. The underlying file to which the alias refers is unchanged.

[Example 6](#) drops an alias.

[Example 7](#) fails because it attempts to drop a system-generated file name and this syntax is not allowed.

Example 6 Dropping an alias name for an Oracle ASM file name

```
ALTER DISKGROUP data DROP ALIAS '+data/payroll/compensation.dbf';
```

Example 7 Dropping an alias name for an Oracle ASM file name

```
ALTER DISKGROUP data
  DROP ALIAS '+data/orcl/datafile/mytable.342.123456789';
```

Dropping Files and Associated Aliases from a Disk Group

You can delete Oracle ASM files and their associated aliases from a disk group using the `DROP FILE` clause of the `ALTER DISKGROUP` statement. You must use a fully qualified file name, or an alias name when specifying the file to delete. The underlying file on the file system is not dropped when the alias is dropped.

Some reasons why you may want to delete files include:

- A file created using aliases is not an Oracle Managed File. Consequently, it is not automatically deleted.
- A point-in-time-recovery of a database might restore the database to a time before a tablespace was created. The restore does not delete the tablespace, but there is no reference to the tablespace or its data file in the restored database. You could manually delete the data file.

In [Example 8](#), the alias name for the file is used when deleting both the file and the alias from a disk group.

In [Example 9](#), the Oracle Managed Files (system-generated) file name is used when dropping the file and any associated alias.

Example 8 Dropping a file and alias from a disk group using the alias name

```
ALTER DISKGROUP data DROP FILE '+data/payroll/compensation.dbf';
```

Example 9 Dropping a file and alias from a disk group using the system-generated name

```
ALTER DISKGROUP data
  DROP FILE '+data/orcl/datafile/mytable.342.123456789';
```

Managing Disk Group Directories

Oracle ASM disk groups contain a system-generated hierarchical directory structure for storing Oracle ASM files. The system-generated file name that Oracle ASM assigns to each file represents a path in this directory hierarchy. The following is an example of a system-generated file name:

```
+data/orcl/CONTROLFILE/Current.256.541956473
```


The plus sign represents the root of the Oracle ASM file system. The `data` directory is the parent directory for all files in the `data` disk group. The `orcl` directory is the parent directory for all files in the `orcl` database, and the `CONTROLFILE` directory contains all control files for the `orcl` database.

You can create your own directories within this hierarchy to store aliases that you create. Thus, in addition to having user-friendly alias names for Oracle ASM files, you can have user-friendly paths to those names.

This section describes how to use the `ALTER DISKGROUP` statement to create a directory structure for aliases. It also describes how you can rename a directory or drop a directory. This section contains the following topics:

- [Creating a Directory](#)
- [Renaming a Directory](#)
- [Dropping a Directory](#)

Creating a Directory

Use the `ADD DIRECTORY` clause of the `ALTER DISKGROUP` statement to create a hierarchical directory structure for alias names for Oracle ASM files. Use the slash (/) or backslash (\) character to separate components of the directory path. The directory path must start with the disk group name, preceded by a plus sign (+), followed by any subdirectory names of your choice.

The parent directory must exist before attempting to create a subdirectory or alias in that directory. A directory must be created below the disk group level.

[Example 10](#) creates a hierarchical directory for disk group `data`, which can contain, for example, the alias name `+data/orcl/control_file1`.

Assuming no subdirectory exists under the directory `+data/orcl`, the SQL statement fails in [Example 11](#).

Example 10 *Creating a new directory*

```
ALTER DISKGROUP data ADD DIRECTORY '+data/orcl';
```

Example 11 *Creating a new subdirectory*

```
ALTER DISKGROUP data
  ADD DIRECTORY '+data/orcl/first_dir/second_dir';
```

Renaming a Directory

The `RENAME DIRECTORY` clause of the `ALTER DISKGROUP` statement enables you to rename a directory. System-created directories (those containing system-generated names) cannot be renamed. The root level (disk group name) cannot be renamed.

[Example 12](#) renames a directory.

Example 12 *Renaming a directory*

```
ALTER DISKGROUP data RENAME DIRECTORY '+data/mydir'
  TO '+data/yourdir';
```

Dropping a Directory

You can delete a directory using the `DROP DIRECTORY` clause of the `ALTER DISKGROUP` statement. You cannot drop a system-created directory. You cannot drop a directory containing alias names unless you also specify the `FORCE` clause.

[Example 13](#) deletes a directory along with its contents.

Example 13 Dropping a directory

```
ALTER DISKGROUP data DROP DIRECTORY '+data/yourdir' FORCE;
```

Accessing Oracle ASM Files with the XML DB Virtual Folder

Oracle ASM files and directories can be accessed through a virtual folder in the XML DB repository. The repository path to the virtual folder is `/sys/asm`. The folder is virtual because its contents do not actually reside in the repository; they exist as normal Oracle ASM files and directories. For example, `/sys/asm` provides a means to access and manipulate the Oracle ASM files and directories with programmatic APIs such as the `DBMS_XDB` package and with XML DB protocols such as FTP and HTTP/WebDAV. You can also use the `ASMCMD cp` command to copy files. See “[cp](#)”.

A typical use for this capability might be to view `/sys/asm` as a Web Folder in a graphical user interface (with the WebDAV protocol), and then copy a Data Pump dumpset from an Oracle ASM disk group to an operating system file system by dragging and dropping.

You must log in as a user other than `SYS` and you must have been granted the `DBA` role to access `/sys/asm` with XML DB protocols. For additional information about the `/sys/asm` folder, refer to “[Inside /sys/asm](#)”.

Note:

For security reasons, FTP is disabled, by default. This is because the IETF FTP protocol specification requires that passwords be transmitted in clear text. Disabling is done by configuring the FTP server port as zero (0). To enable FTP, set the `ftp-port` parameter to the FTP port to use, such as 2100.

See Also:

- *Oracle XML DB Developer's Guide* for information about Oracle XML DB, including additional ways to configure port numbers for the XML DB protocol servers
 - *Oracle Database PL/SQL Packages and Types Reference* for information about the `DBMS_XDB` package
-
-

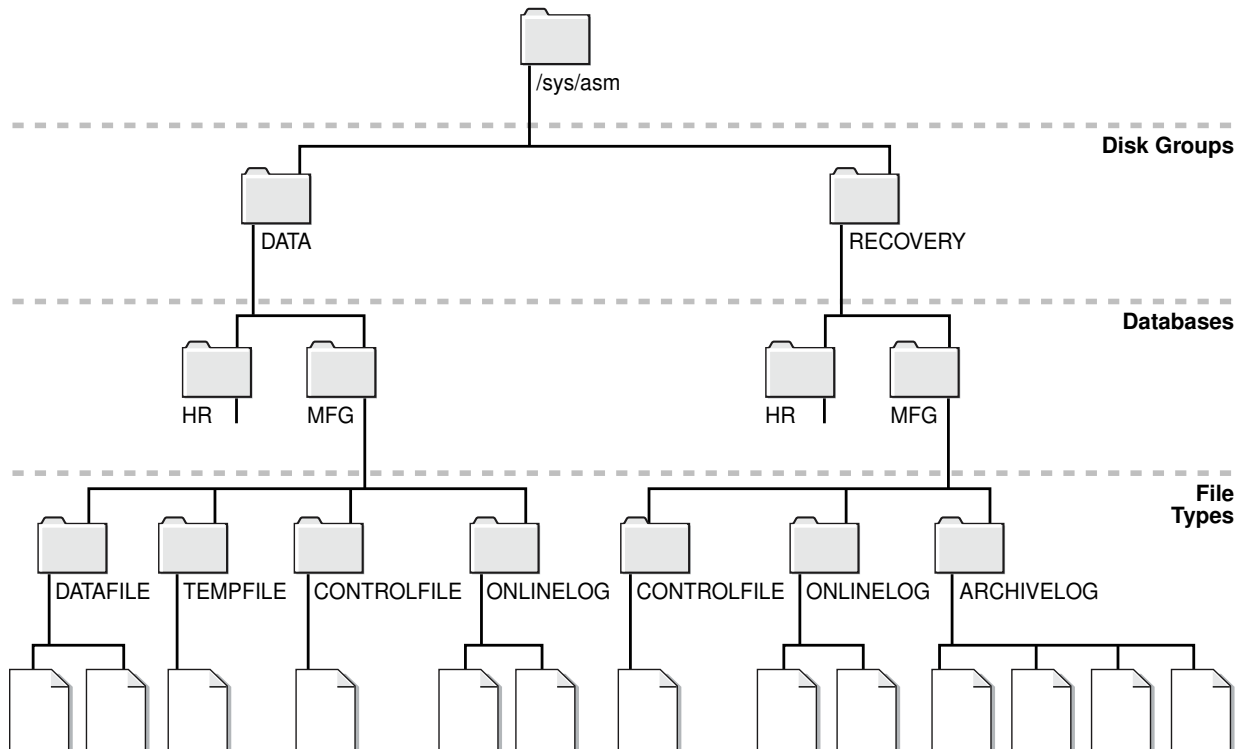
Inside /sys/asm

The Oracle ASM virtual folder is created by default during XML DB installation. If the database is not configured to use Oracle ASM, the folder is empty and no operations are permitted on it.

The Oracle ASM virtual folder contains folders and subfolders that follow the hierarchy defined by the structure of an Oracle ASM fully qualified file name. [Figure 1](#) illustrates an example of this hierarchy, which for simplicity, excludes directories created for aliases.

The folder `/sys/asm` contains one subfolder for every mounted disk group, and each disk group folder contains one subfolder for each database that uses the disk group. In addition, a disk group folder might contain files and folders corresponding to aliases created by the administrator. Continuing the hierarchy, the database folders contain file type folders, which contain the Oracle ASM files.

Figure 1 Hierarchical Structure of Oracle ASM Folders in an XML DB Installation



The following are usage restrictions on `/sys/asm`:

- You cannot create hard links to existing Oracle ASM files or directories with APIs such as `DBMS_XDB.LINK`.
- You cannot rename (move) an Oracle ASM file to another disk group or to a directory outside Oracle ASM.

You can use the directory `/sys/asm` for storing the names of disk groups. You cannot store other files in this directory. Within the disk group directories under `/sys/asm`, such as `/sys/asm/DATA`, you can only store database files in these sub-directories. Oracle ASM rejects attempts to store non-database files in these directories.

Using DBMS_FILE Transfer Utility for Oracle ASM

The `DBMS_FILE_TRANSFER` package provides procedures to copy Oracle ASM files within a database or to transfer binary files between databases that use Oracle ASM. The `DBMS_FILE_TRANSFER` package has the following procedures:

- `COPY_FILE`—Reads a file from a source directory and creates a copy of the file in a destination directory. The source and destination directories can both be in a local file system or in an Oracle ASM disk group. You can also use this procedure to copy between a local file system and an Oracle ASM disk group; the copy operation is valid in either direction.
- `GET_FILE`—Contacts a remote database to read a remote file and then creates a copy of the file in the local file system or Oracle ASM disk group.
- `PUT_FILE`—Reads a local file or Oracle ASM disk group and contacts a remote database to create a copy of the file in the remote file system.

See Also:

Oracle Database PL/SQL Packages and Types Reference for more information about the `DBMS_FILE_TRANSFER` package

Managing Disk Group Templates

This section describes how to manage disk group templates under the following topics:

- [Template Attributes](#)
- [Adding Templates to a Disk Group](#)
- [Modifying a Disk Group Template](#)
- [Dropping Templates from a Disk Group](#)
- [Creating Tablespaces in Oracle ASM: Specifying Attributes with Templates](#)

Templates are used to set attributes of files created in an Oracle ASM disk group. When a file is created, redundancy and striping attributes are set for that file based on an explicitly named template or the system template that is the default template for the file type.

When a disk group is created, Oracle ASM creates a set of default templates for that disk group. The set consists of one template for each file type (data file, control file, redo log file, and so on) that is supported by Oracle ASM. For example, a template named `ONLINELOG` provides the default file redundancy and striping attributes for all redo log files written to Oracle ASM disks. Default template settings depend on the disk group type. The default template for data files for a normal redundancy disk group sets two-way mirroring, while the corresponding default template in a high redundancy disk group sets three-way mirroring. You can modify these default templates.

For example, default redundancy for the online redo log files (`ONLINELOG` template) for a normal redundancy disk group is `MIRROR`. In [Example 1](#), this setting means that when one copy of a redo log file extent is written to a disk in failure group `controller1`, a mirrored copy of the file extent is written to a disk in failure group `controller2`. To support the default mirroring of a normal redundancy disk group, at least two failure groups must be defined.

[Table 6](#) lists the default templates and the attributes that are associated to matching files. As the table shows, the initial redundancy value of each default template depends on the type of disk group that the template belongs to.

Using clauses of the `ALTER DISKGROUP` statement, you can add new templates to a disk group, modify existing ones, or drop templates. The reason to add templates is to create the right combination of attributes to meet unique requirements. You can then reference a template name when creating a file, thereby assigning desired attributes based on an individual file rather than on the file type.

The `V$ASM_TEMPLATE` view lists all of the templates known to the Oracle ASM instance. For an example of the information displayed in the `V$ASM_TEMPLATE` view, see [Example 10](#).

Template Attributes

[Table 4](#) shows the permitted striping attribute values and allocation unit size chunks. These values correspond to the `STRIPE` column of `V$ASM_TEMPLATE`.

Table 4 Permitted values for Oracle ASM template striping attribute

Striping Attribute Value	Description
FINE	Striping in 128 KB chunks.
COARSE	Striping in 1 MB chunks.

[Table 5](#) shows the permitted redundancy values for Oracle ASM templates. These values correspond to the `REDUND` column of `V$ASM_TEMPLATE`.

Table 5 Permitted values for Oracle ASM template redundancy attribute

Redundancy Attribute Value	Resulting Mirroring in Normal Redundancy Disk Group	Resulting Mirroring in High Redundancy Disk Group	Resulting Mirroring in External Redundancy Disk Group
MIRROR	Two-way mirroring	Three-way mirroring	(Not allowed)
HIGH	Three-way mirroring	Three-way mirroring	(Not allowed)
UNPROTECTED	No mirroring	(Not allowed)	No mirroring

[Table 6](#) shows the initial attribute settings for some default templates. The type of mirroring associated with the **Mirroring** column for normal, high, and external redundancy disk groups is specified in [Table 5](#). For example, the **Mirror** column for high redundancy disk groups displays `MIRROR` in [Table 6](#). In [Table 5](#), the `MIRROR` value for high redundancy disk groups corresponds to Three-way mirroring.

For an example of the output of the `V$ASM_TEMPLATE` view, refer to [Example 10](#).

Table 6 Oracle ASM system default templates attribute settings

Template Name	File Striping	Mirroring, Normal Redundancy Disk Group	Mirroring, High Redundancy Disk Group	Mirroring, External Redundancy Disk Group	Primary Region	Mirror Region
ARCHIVELOG	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
ASMPARAMETERFILE	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
AUDIT_SPILLFILES	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
AUTOBACKUP	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
BACKUPSET	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
CHANGETRACKING	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD

Template Name	File Striping	Mirroring, Normal Redundancy Disk Group	Mirroring, High Redundancy Disk Group	Mirroring, External Redundancy Disk Group	Primary Region	Mirror Region
CONTROLFILE	FINE	HIGH	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
DATAFILE	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
DATAGUARDCONFIG	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
DUMPSET	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
FLASHBACK	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
FLASHFILE	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
KEY_STORE	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
OCRFILE	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
ONLINELOG	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
PARAMETERFILE	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
TEMPFILE	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
VOTINGFILE	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD
XTRANSPORT	COARSE	MIRROR	MIRROR	UNPROTECTED	COLD	MIRRORCOLD

Table 7 shows the permitted primary and mirror region values for Oracle ASM templates. These values correspond to the PRIMARY_REGION and MIRROR_REGION columns of V\$ASM_TEMPLATE. For more information about disk regions, see “Intelligent Data Placement”.

Table 7 Permitted values for Oracle ASM template primary and mirror region attribute

Primary and Mirror Region Attribute Value	Description
COLD, MIRRORCOLD	Use the inner most tracks (closest to spindle) on the disk drive.
HOT, MIRRORHOT	Use the outermost tracks which have greater speed and higher bandwidth.

Adding Templates to a Disk Group

To add a template to a disk group, use the ADD TEMPLATE clause of the ALTER DISKGROUP statement.

If the name of your new template is not listed in Table 6, then it is not used as a default template for database file types. To use the template, you must reference its name when creating a file.

When adding a template to a disk group, the attributes are optional. If no redundancy attribute is specified, then the value defaults to MIRROR for a normal redundancy disk group, HIGH for a high redundancy disk group, and UNPROTECTED for an external redundancy disk group. If you do not specify a striping attribute, then the value defaults to COARSE. If you do not specify a value for the primary or mirror region attributes, then the value defaults to COLD and MIRRORCOLD respectively.

[Example 14](#) creates a new template named `reliable` for the normal redundancy disk group data.

[Example 15](#) creates a new template named `unreliable` that specifies `UNPROTECTED` (no mirroring) for files.

Note:

Oracle discourages using unprotected files unless you have implemented hardware mirroring. The previous example is presented only to further illustrate how the attributes for templates are set.

See Also:

Oracle Database SQL Language Reference for more information about the `ALTER DISKGROUP...ADD TEMPLATE` command

Example 14 Adding a template with high redundancy to a disk group

```
ALTER DISKGROUP data ADD TEMPLATE reliable ATTRIBUTES (HIGH FINE);
```

Example 15 Adding a template with external redundancy to a disk group

```
ALTER DISKGROUP data ADD TEMPLATE unreliable ATTRIBUTES (UNPROTECTED);
```

Modifying a Disk Group Template

The `MODIFY TEMPLATE` clause of the `ALTER DISKGROUP` statement enables you to modify the attribute specifications of an existing system default or user-defined disk group template. Only specified template attributes are changed. Unspecified properties retain their current value. When you modify an existing template, only new files created by the template reflect the attribute changes. Existing files maintain their attributes.

[Example 16](#) changes the striping attribute specification of the `reliable` template for disk group data.

Example 16 Modifying a disk group template

```
ALTER DISKGROUP data MODIFY TEMPLATE reliable
  ATTRIBUTES (COARSE);
```

Dropping Templates from a Disk Group

Use the `DROP TEMPLATE` clause of the `ALTER DISKGROUP` statement to drop one or more templates from a disk group. You can only drop templates that are user-defined; you cannot drop system default templates.

[Example 17](#) drops the previously created template `unreliable` from data:

Example 17 Dropping a template from a disk group

```
ALTER DISKGROUP data DROP TEMPLATE unreliable;
```

Creating Tablespaces in Oracle ASM: Specifying Attributes with Templates

Use the SQL `ALTER SYSTEM` and `CREATE TABLESPACE` statements to create a tablespace that uses a user-defined template to specify the attributes of the data file.

[Example 18](#) assumes that the template (`mytemplate`) has been defined.

Example 18 *Using a user-defined template to specify attributes*

```
ALTER SYSTEM SET DB_CREATE_FILE_DEST = '+data(mytemplate)';  
  
CREATE TABLESPACE mytblspace;
```

Using Views to Display Oracle ASM Information

This chapter contains information about using dynamic views to display Oracle Automatic Storage Management (Oracle ASM) information.

- [Views Containing Oracle ASM Disk Group Information](#)
- [Viewing Oracle ASM File Access Control Information](#)
- [Viewing Disk Region Information](#)

See Also:

Oracle Database Reference for information about all of the V\$ASM* dynamic performance views

Views Containing Oracle ASM Disk Group Information

You can use the views in [Table 1](#) to obtain information about Oracle ASM disk groups.

Table 1 Oracle ASM dynamic views for disk group information

View	Description
V\$ASM_ALIAS	Contains one row for every alias present in every disk group mounted by the Oracle ASM instance.
V\$ASM_ATTRIBUTE	Displays one row for each attribute defined. In addition to attributes specified by CREATE DISKGROUP and ALTER DISKGROUP statements, the view may show other attributes that are created automatically. Attributes are only displayed for disk groups where COMPATIBLE . ASM is set to 11 . 1 or higher.
V\$ASM_AUDIT_CLEAN_EVENTS	Displays information about the history of audit trail cleanup or purge events.
V\$ASM_AUDIT_CLEANUP_JOBS	Displays information about the configured audit trail purge jobs.
V\$ASM_AUDIT_CONFIG_PARAMS	Displays information about the currently configured audit trail properties.
V\$ASM_AUDIT_LAST_ARCH_TS	Displays information about the last archive timestamps set for audit trail cleanup or purges.
V\$ASM_CLIENT	In an Oracle ASM instance, identifies databases using disk groups managed by the Oracle ASM instance. In an Oracle Database instance, contains information about the Oracle ASM instance if the database has any open Oracle ASM files.

View	Description
V\$ASM_DISK	Contains one row for every disk discovered by the Oracle ASM instance, including disks that are not part of any disk group. This view performs disk discovery every time it is queried.
V\$ASM_DISK_IOSTAT	Displays information about disk I/O statistics for each Oracle ASM client. In an Oracle Database instance, only the rows for that instance are shown.
V\$ASM_DISK_STAT	Contains the same columns as V\$ASM_DISK, but to reduce overhead, does not perform a discovery when it is queried. It only returns information about any disks that are part of mounted disk groups in the storage system. To see all disks, use V\$ASM_DISK instead.
V\$ASM_DISKGROUP	Describes a disk group (number, name, size related info, state, and redundancy type). This view performs disk discovery every time it is queried.
V\$ASM_DISKGROUP_STAT	Contains the same columns as V\$ASM_DISKGROUP, but to reduce overhead, this view does not perform a discovery when it is queried. To see more complete information on all disks, use V\$ASM_DISKGROUP.
V\$ASM_ESTIMATE	Displays an estimate of the work involved in execution plans for Oracle ASM disk group rebalance and resync operations.
V\$ASM_FILE	Contains one row for every Oracle ASM file in every disk group mounted by the Oracle ASM instance.
V\$ASM_OPERATION	In an Oracle ASM instance, contains one row for every active Oracle ASM long running operation executing in the Oracle ASM instance. In an Oracle Database instance, contains no rows.
V\$ASM_TEMPLATE	Contains one row for every template present in every disk group mounted by the Oracle ASM instance.
V\$ASM_USER	Contains the effective operating system user names of connected database instances and names of file owners.
V\$ASM_USERGROUP	Contains the creator for each Oracle ASM File Access Control group.
V\$ASM_USERGROUP_MEMBER	Contains the members for each Oracle ASM File Access Control group.

When querying V\$ASM views, the value of the disk group number is not a static value. When a disk group is mounted, a disk group number is chosen. This number may change across disk group mounts. A disk group number is not recorded in any persistent structure, but the current value can be viewed in the GROUP_NUMBER column of the V\$ASM views.

An example of the use of the V\$ASM_ATTRIBUTE and V\$ASM_DISKGROUP views is shown in [Example 1](#). The COMPATIBLE.ASM value must be set to 11.1 or higher for the disk group to display in the V\$ASM_ATTRIBUTE view output. Attributes that are designated as read-only (Y) can only be set during disk group creation.

You can view the compatibility for a disk group with the V\$ASM_DISKGROUP view, as shown in [Example 2](#).

An example of the use of the V\$ASM_DISK and V\$ASM_DISKGROUP views is shown in [Example 3](#). This example displays the disks associated with a disk group, plus the mount status, state, and failure group of the disks.

An example of the use of the V\$ASM_CLIENT and V\$ASM_DISKGROUP views on an Oracle ASM instance is shown in [Example 4](#). This example displays disk groups with information about the connected database client instances.

Example 1 Viewing disk group attributes with V\$ASM_ATTRIBUTE

```
SELECT SUBSTR(dg.name,1,12) AS diskgroup, SUBSTR(a.name,1,24) AS name,
       SUBSTR(a.value,1,24) AS value, read_only FROM V$ASM_DISKGROUP dg,
       V$ASM_ATTRIBUTE a WHERE dg.name = 'DATA' AND dg.group_number =
a.group_number
       AND a.name NOT LIKE '%template%';
```

DISKGROUP	NAME	VALUE	READ_ON
DATA	thin_provisioned	FALSE	N
DATA	access_control.umask	066	N
DATA	phys_meta_replicated	true	Y
DATA	disk_repair_time	3.6h	N
DATA	idp.boundary	auto	N
DATA	idp.type	dynamic	N
DATA	content.type	data	N
DATA	content.check	FALSE	N
DATA	au_size	1048576	Y
DATA	sector_size	512	Y
DATA	compatible.asm	12.1.0.0.0	N
DATA	compatible.rdbms	12.1.0.0.0	N
DATA	compatible.advm	12.1.0.0.0	N
DATA	cell.smart_scan_capable	FALSE	N
DATA	access_control.enabled	FALSE	N
DATA	failgroup_repair_time	24.0h	N

Example 2 Viewing the compatibility of a disk group with V\$ASM_DISKGROUP

```
SELECT name AS diskgroup, substr(compatibility,1,12) AS asm_compat,
       substr(database_compatibility,1,12) AS db_compat FROM V$ASM_DISKGROUP;
```

DISKGROUP	ASM_COMPAT	DB_COMPAT
DATA	12.1.0.0.0	12.1.0.0.0
FRA	12.1.0.0.0	12.1.0.0.0

Example 3 Viewing disks in disk groups with V\$ASM_DISK

```
SELECT SUBSTR(dg.name,1,16) AS diskgroup, SUBSTR(d.name,1,16) AS asmdisk,
       d.mount_status, d.state, SUBSTR(d.failgroup,1,16) AS failgroup
FROM V$ASM_DISKGROUP dg, V$ASM_DISK d WHERE dg.group_number =
d.group_number;
```

DISKGROUP	ASMDISK	MOUNT_S	STATE	FAILGROUP
DATA	DATA_0000	CACHED	NORMAL	DATA_0000
DATA	DATA_0010	CACHED	NORMAL	DATA_0010
DATA	DATA_0001	CACHED	NORMAL	DATA_0001
DATA	DATA_0003	CACHED	NORMAL	DATA_0003
DATA	DATA_0009	CACHED	NORMAL	DATA_0009
DATA	DATA_0007	CACHED	NORMAL	DATA_0007
DATA	DATA_0004	CACHED	NORMAL	DATA_0004
DATA	DATA_0008	CACHED	NORMAL	DATA_0008
DATA	DATA_0006	CACHED	NORMAL	DATA_0006
DATA	DATA_0011	CACHED	NORMAL	DATA_0011
DATA	DATA_0005	CACHED	NORMAL	DATA_0005
DATA	DATA_0002	CACHED	NORMAL	DATA_0002
FRA	FRA_0011	CACHED	NORMAL	FRA_0011
FRA	FRA_0002	CACHED	NORMAL	FRA_0002
FRA	FRA_0001	CACHED	NORMAL	FRA_0001
FRA	FRA_0003	CACHED	NORMAL	FRA_0003
FRA	FRA_0004	CACHED	NORMAL	FRA_0004

```
FRA          FRA_0000          CACHED  NORMAL  FRA_0000
...
```

Example 4 Viewing disk group clients with V\$ASM_CLIENT

```
SELECT dg.name AS diskgroup, SUBSTR(c.instance_name,1,12) AS instance,
       SUBSTR(c.db_name,1,12) AS dbname, SUBSTR(c.SOFTWARE_VERSION,1,12) AS
software,
       SUBSTR(c.COMPATIBLE_VERSION,1,12) AS compatible
FROM V$ASM_DISKGROUP dg, V$ASM_CLIENT c
WHERE dg.group_number = c.group_number;
```

DISKGROUP	INSTANCE	DBNAME	SOFTWARE	COMPATIBLE
DATA	+ASM	+ASM	12.1.0.1.0	12.1.0.1.0
DATA	orcl	orcl	12.1.0.1.0	12.1.0.1.0
DATA	+ASM	asmvol	12.1.0.1.0	12.1.0.1.0
FRA	orcl	orcl	12.1.0.1.0	12.1.0.1.0
...				

Viewing Oracle ASM File Access Control Information

You can view information about Oracle ASM File Access Control in the columns of the V\$ASM_USER, V\$ASM_USERGROUP, V\$ASM_USERGROUP_MEMBER, and V\$ASM_FILE views.

Example 5 shows information about Oracle ASM File Access Control users displayed in the V\$ASM_USER view.

Example 6 shows information about Oracle ASM File Access Control user groups displayed in the V\$ASM_USERGROUP view.

Example 7 shows information about Oracle ASM File Access Control user groups and members displayed in the V\$ASM_USERGROUP_MEMBER view.

Example 8 shows information about Oracle ASM File Access Control file permissions displayed in the V\$ASM_FILE view.

For more information about Oracle ASM File Access Control, see [“Managing Oracle ASM File Access Control for Disk Groups”](#).

Example 5 Viewing Oracle ASM File Access Control information with V\$ASM_USER

```
SELECT dg.name AS diskgroup, u.group_number, u.user_number, u.os_id, u.os_name
FROM V$ASM_DISKGROUP dg, V$ASM_USER u
WHERE dg.group_number = u.group_number AND dg.name = 'DATA';
```

DISKGROUP	GROUP_NUMBER	USER_NUMBER	OS_ID	OS_NAME
DATA	1	1 1001	oracle1	
DATA	1	2 1002	oracle2	
DATA	1	3 1003	grid	

Example 6 Viewing File Access Control information with V\$ASM_USERGROUP

```
SELECT dg.name AS diskgroup, ug.group_number, ug.owner_number, u.os_name,
       ug.usergroup_number, ug.name FROM V$ASM_DISKGROUP dg, V$ASM_USER u, V$ASM_USERGROUP ug
WHERE dg.group_number = ug.group_number AND dg.name = 'DATA'
AND ug.owner_number = u.user_number;
```

DISKGROUP	GROUP_NUMBER	OWNER_NUMBER	OS_NAME	USERGROUP_NUMBER	NAME
DATA	1	3	grid	1	asm_data

Example 7 Viewing File Access Control information with V\$ASM_USERGROUP_MEMBER

```
SELECT dg.name AS diskgroup, um.group_number, um.member_number, u.os_name,
       um.usergroup_number, ug.name FROM V$ASM_DISKGROUP dg, V$ASM_USER u, V$ASM_USERGROUP_MEMBER
um,
       V$ASM_USERGROUP ug WHERE dg.group_number = um.group_number AND
       dg.group_number = ug.group_number AND dg.group_number = u.group_number AND dg.name =
'DATA'
       AND um.member_number = u.user_number AND um.usergroup_number = ug.usergroup_number;
```

DISKGROUP	GROUP_NUMBER	MEMBER_NUMBER	OS_NAME	USERGROUP_NUMBER	NAME
DATA	1	1	oracle1	1	asm_data
DATA	1	2	oracle2	1	asm_data

Example 8 Viewing Oracle ASM File Access Control information with V\$ASM_FILE

```
SELECT dg.name AS diskgroup, a.name, f.permissions, f.user_number, u.os_name,
       f.usergroup_number, ug.name
FROM V$ASM_DISKGROUP dg, V$ASM_USER u, V$ASM_USERGROUP ug, V$ASM_FILE f, V$ASM_ALIAS a
WHERE dg.name = 'FRA' AND dg.group_number = u.group_number AND
       u.group_number = ug.group_number AND ug.group_number = f.group_number AND
       f.group_number = a.group_number AND
       f.usergroup_number = ug.usergroup_number AND f.user_number = u.user_number AND
       f.file_number = a.file_number;
```

DISKGROUP	NAME	PERMISSIONS	USER_NUMBER	OS_NAME	USERGROUP_NUMBER	NAME
DATA	USERS.259.685366091	rw-r-----	3	grid	1	asm_fra
DATA	TEMP.264.685366227	rw-r-----	3	grid	1	asm_fra
...						

Viewing Disk Region Information

Information about Intelligent Data Placement is displayed in the columns of the V\$ASM_DISK, V\$ASM_DISK_IOSTAT, V\$ASM_FILE, and V\$ASM_TEMPLATE views.

[Example 9](#) shows queries for Intelligent Data Placement information in the PRIMARY_REGION and MIRROR_REGION columns of the V\$ASM_FILE view.

[Example 10](#) displays Intelligent Data Placement information in the PRIMARY_REGION and MIRROR_REGION columns of the V\$ASM_TEMPLATE view.

For information about setting Intelligent Data Placement, see [“Intelligent Data Placement”](#).

Example 9 Viewing Intelligent Data Placement information with V\$ASM_FILE

```
SELECT dg.name AS diskgroup, f.file_number, f.primary_region, f.mirror_region, f.hot_reads,
       f.hot_writes, f.cold_reads, f.cold_writes
FROM V$ASM_DISKGROUP dg, V$ASM_FILE f
WHERE dg.group_number = f.group_number and dg.name = 'DATA';
```

DISKGROUP	FILE_NUMBER	PRIM	MIRR	HOT_READS	HOT_WRITES	COLD_READS	COLD_WRITES
DATA	257	COLD	COLD	0	0	119770	886575
DATA	258	COLD	COLD	0	0	1396	222282
DATA	259	COLD	COLD	0	0	2056	199
DATA	260	COLD	COLD	0	0	42377	1331016
DATA	261	COLD	COLD	0	0	4336300	1331027
...							

**Example 10 Viewing Intelligent Data Placement information with V
\$ASM_TEMPLATE**

```
SELECT dg.name AS diskgroup, t.name, t.stripe, t.redundancy, t.primary_region, t.mirror_region
FROM V$ASM_DISKGROUP dg, V$ASM_TEMPLATE t
WHERE dg.group_number = t.group_number and dg.name = 'DATA' ORDER BY t.name;
```

DISKGROUP	NAME	STRIPE	REDUND	PRIM	MIRR
DATA	ARCHIVELOG	COARSE	MIRROR	COLD	COLD
DATA	ASMPARAMETERFILE	COARSE	MIRROR	COLD	COLD
DATA	AUDIT_SPILLFILES	COARSE	MIRROR	COLD	COLD
DATA	AUTOBACKUP	COARSE	MIRROR	COLD	COLD
DATA	AUTOLOGIN_KEY_STORE	COARSE	MIRROR	COLD	COLD
DATA	BACKUPSET	COARSE	MIRROR	COLD	COLD
DATA	CHANGETRACKING	COARSE	MIRROR	COLD	COLD
DATA	CONTROLFILE	FINE	HIGH	COLD	COLD
DATA	DATAFILE	COARSE	MIRROR	COLD	COLD
DATA	DATAGUARDCONFIG	COARSE	MIRROR	COLD	COLD
DATA	DUMPSET	COARSE	MIRROR	COLD	COLD
DATA	FLASHBACK	COARSE	MIRROR	COLD	COLD
DATA	FLASHFILE	COARSE	MIRROR	COLD	COLD
DATA	INCR XTRANSPORT BACKUPSET	COARSE	MIRROR	COLD	COLD
DATA	KEY_STORE	COARSE	MIRROR	COLD	COLD
DATA	OCRFILE	COARSE	MIRROR	COLD	COLD
DATA	ONLINELOG	COARSE	MIRROR	COLD	COLD
DATA	PARAMETERFILE	COARSE	MIRROR	COLD	COLD
DATA	TEMPFILE	COARSE	MIRROR	COLD	COLD
DATA	VOTINGFILE	COARSE	MIRROR	COLD	COLD
DATA	XTRANSPORT	COARSE	MIRROR	COLD	COLD
DATA	XTRANSPORT BACKUPSET	COARSE	MIRROR	COLD	COLD

22 rows selected.

Administering Oracle ASM with Oracle Enterprise Manager

This chapter describes how to administer Oracle Automatic Storage Management (Oracle ASM) with Oracle Enterprise Manager Cloud Control.

This chapter contains the following topics:

- [Accessing the Oracle Automatic Storage Management Home Page](#)
- [Configuring Oracle ASM Initialization Parameters with Oracle Enterprise Manager](#)
- [Managing Oracle ASM Users with Oracle Enterprise Manager](#)
- [Managing Disk Groups with Oracle Enterprise Manager](#)
- [Managing Oracle ASM File Access Control with Oracle Enterprise Manager](#)
- [Managing Directories_ Files_ and Aliases with Oracle Enterprise Manager](#)
- [Managing Disk Group Templates with Oracle Enterprise Manager](#)
- [Managing Oracle ASM Filter Driver With Oracle Enterprise Manager](#)
- [Monitoring Oracle ASM Performance With Oracle Enterprise Manager](#)
- [Backing Up Oracle ASM Files with Oracle Enterprise Manager](#)
- [Performing Bad Block Recovery with Oracle Enterprise Manager](#)
- [Migrating to Oracle ASM with Oracle Enterprise Manager](#)
- [Monitoring Alerts and Incidents With Oracle ASM Support Workbench](#)
- [Monitoring Oracle Flex ASM](#)

See Also:

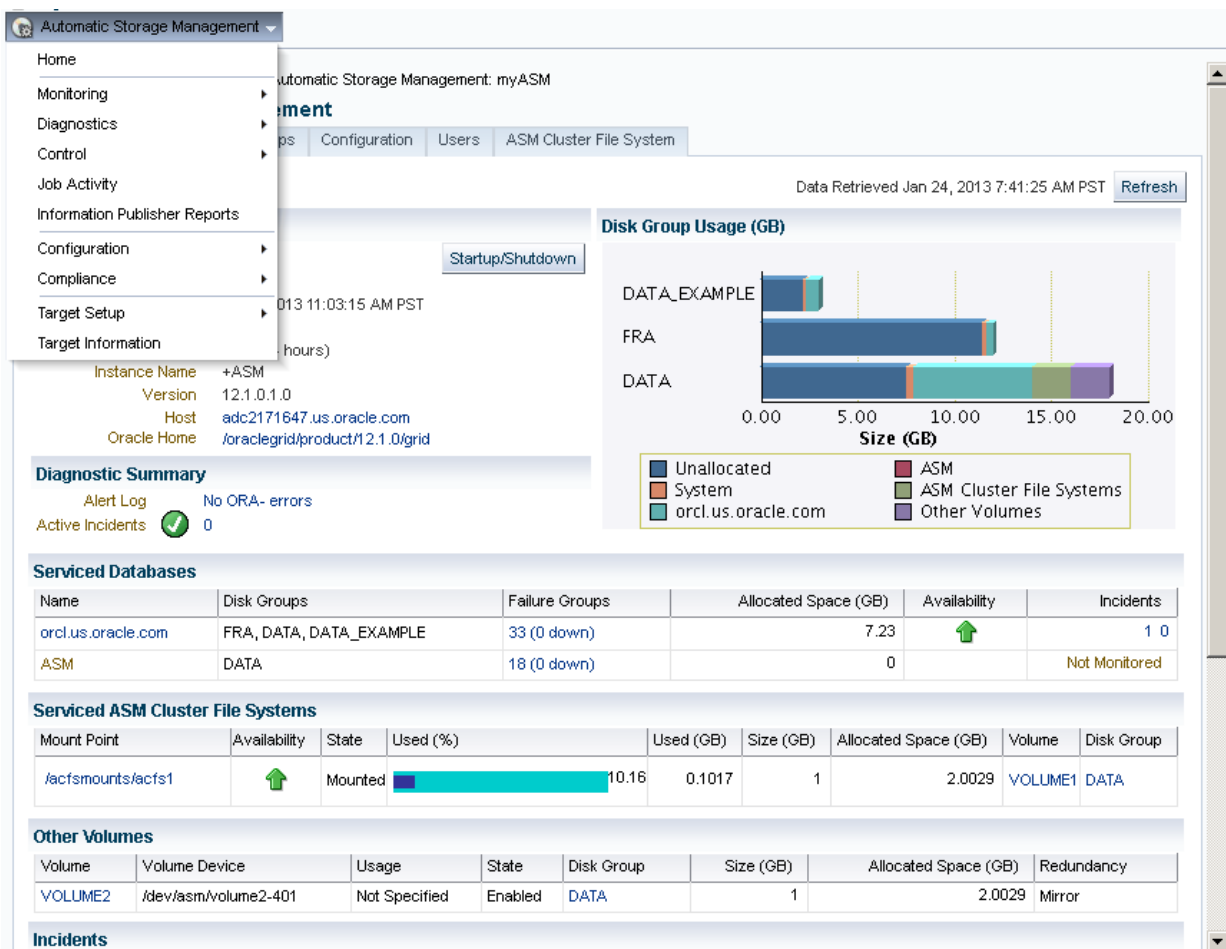
- *Oracle Enterprise Manager Cloud Administration Guide*
 - *Oracle Enterprise Manager Administration*
-

Accessing the Oracle Automatic Storage Management Home Page

All Oracle ASM administration tasks begin with the Oracle Automatic Storage Management home page in Oracle Enterprise Manager Cloud Control, similar to the graphic shown in [Figure 1](#) . The Oracle Automatic Storage Management home page displays:

- The status of the Oracle ASM instance.
- A chart that shows the used and free space of each disk group and disk group internal usage.
- A list of databases that are serviced by the Oracle ASM instance.
- A list of Oracle Automatic Storage Management Cluster File System (Oracle ACFS) file systems that are serviced by the Oracle ASM instance.
- A list of other non-Oracle ACFS volumes.
- A list of alerts for the Oracle ASM instance and the host computer.
- Links to the Oracle ASM Performance, Disk Groups, Configuration, Users, and Oracle ACFS pages.

Figure 1 Oracle Automatic Storage Management Home Page



To access the Oracle Automatic Storage Management home page on a single-instance system:

1. Log in to Oracle Enterprise Manager Cloud Control.
2. Under the **Targets** drop down menu at the top of the page, select **All Targets**.
3. In the lists of targets on the **All Targets** page, click the target for the Oracle ASM instance.

4. If prompted for Oracle ASM login credentials, then enter the user `SYS`, provide the `SYS` password that was set for the Oracle ASM instance during installation, and connect as `SYSASM`. The Oracle Automatic Storage Management home page displays similar to the page in [Figure 1](#).

For more information about authentication, refer to “[Authentication for Accessing Oracle ASM Instances](#)”.

Configuring Oracle ASM Initialization Parameters with Oracle Enterprise Manager

You can configure Oracle ASM with the Oracle Enterprise Manager Configuration Parameters page similar to the screen shown in [Figure 2](#).

Figure 2 Oracle Automatic Storage Management Configuration Parameters Page

Configuration

Home Performance Disk Groups **Configuration** Users ASM Cluster File System

Configuration Parameters

Disk Discovery Path Revert Apply
 This path limits the set of disks considered for discovery. It should match the path or the directory containing the disk. e.g. `/dev/raw/*` for Linux based operating systems.

Auto Mount Disk Groups
 The list of the Disk Group names to be mounted by the ASM at startup or when `ALTER DISKGROUP ALL MOUNT` command is used.

Rebalance Power
 Higher values allows the operation to complete more quickly but takes more I/O bandwidth away from the database. Lower values causes rebalance to take longer but leave more I/O bandwidth for the database. Valid values range from 0 to 1024.

Preferred Read Failure Groups
 Specify a comma-separated list of failure groups whose member disks will be preferred read disks for this node. If there is more than one mirror copy to read from, ASM will read from the preferred disk.

To configure the Oracle ASM instance:

1. Access the Oracle Automatic Storage Management home page.
See “[Accessing the Oracle Automatic Storage Management Home Page](#)” for instructions.
2. Click the **Configuration** link at the top of the page to view the Configuration Parameters page.
3. Update the configuration options on the page as follows:
 - Disk Discovery Path (`ASM_DISKSTRING` initialization parameter)
Enter a string value. See “[ASM_DISKSTRING](#)”.
 - Auto Mount Disk Groups (`ASM_DISKGROUPS` initialization parameter)
Enter a string value. See “[ASM_DISKGROUPS](#)”.
 - Rebalance Power (`ASM_POWER_LIMIT` initialization parameter)
Enter an integer value. See “[ASM_POWER_LIMIT](#)”.
 - Preferred Read Failure Groups (Only in Oracle RAC environments)
(`ASM_PREFERRED_READ_FAILURE_GROUPS` initialization parameter)

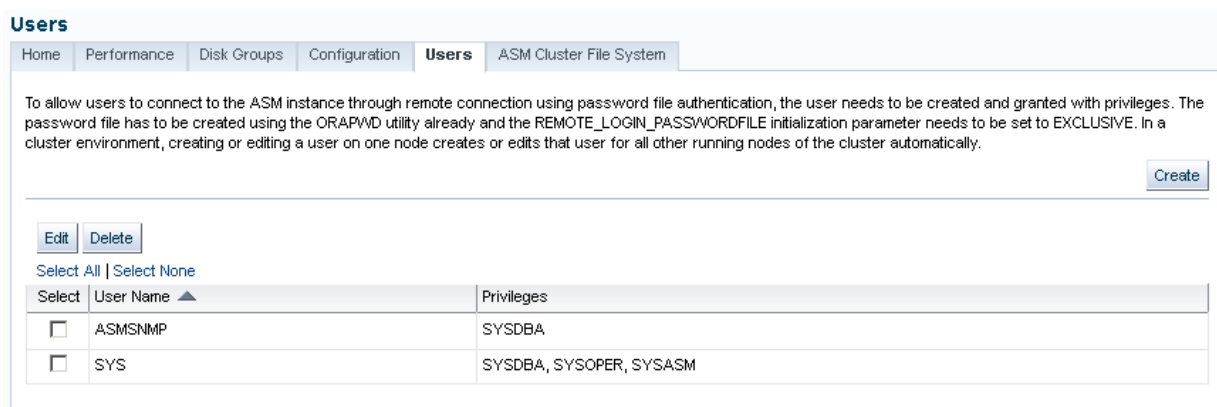
Enter a comma-delimited string of values in which each string represents a failure group. This parameter is generally used only for clustered Oracle ASM instances. See “[ASM_PREFERRED_READ_FAILURE_GROUPS](#)”.

4. Click **Apply** to save your changes or click **Revert** to discard any changes made on the page.

Managing Oracle ASM Users with Oracle Enterprise Manager

You can manage Oracle ASM users with the Oracle Enterprise Manager Users page, shown in [Figure 3](#). Access this page by clicking the Users tab that is near the top center of the Oracle Automatic Storage Management home page.

Figure 3 Oracle Automatic Storage Management Users Page



To manage Oracle ASM users:

1. Access the Oracle Automatic Storage Management home page.
See “[Accessing the Oracle Automatic Storage Management Home Page](#)” for instructions.
2. Click the **Users** link at the top to view the Users property page.
ASMSNMP is a less privileged user that is primarily used by Oracle Enterprise Manager to monitor Oracle ASM instances. This account is granted the SYSDBA privilege. ASMSNMP is created by Oracle ASM Configuration Assistant (ASMCA) when an Oracle ASM instance is created. For information about creating an Oracle ASM instance with ASMCA, see “[Creating Oracle ASM Instances with ASMCA](#)”.

See Also:

- *Oracle Grid Infrastructure Installation Guide* for information about installing Oracle ASM
 - *Oracle Database Installation Guide* for information about reviewing database accounts and passwords
-

3. Click **Create** to add a new Oracle ASM user. When you add users, Oracle Enterprise Manager displays a Create User page in which you must enter user login credentials that include the user name, password, and password confirmation. You can also grant privileges to the new user by selecting privileges

in the Available Privileges column and clicking the right arrow buttons to move privileges to the Granted Privileges column, or move the privilege by double clicking it. The available privileges include SYSDBA, SYSOPER, and SYSASM. Click **OK** to create the user, **Cancel** to cancel the procedure, or **Show SQL** to view the SQL that Oracle Enterprise Manager uses to create the user.

4. To edit a user's properties, select the box in the Select column of the user to edit, then click **Edit**. On the Edit User page, modify the password if needed. You can also alter the privileges that are assigned to the user by selecting the privilege and using the right and left arrow buttons to move the privilege from the Granted Privileges column to the Available Privileges column and vice versa. You can also move the privilege by double clicking it. Click **OK** to edit the user properties, **Revert** to cancel the procedure, or **Show SQL** to view the SQL that Oracle Enterprise Manager uses to edit the user's properties.
5. To delete an Oracle ASM user, select the box in the Select column for the user to delete, then click **Delete**. On the confirmation dialog, click **Yes** to delete the user or **No** to stop the user deletion procedure.

For more information about authentication, refer to “[Authentication for Accessing Oracle ASM Instances](#)”.

Managing Disk Groups with Oracle Enterprise Manager

This section describes how to manage disk groups under the following topics:

- [Creating Disk Groups](#)
- [Adding Disks to Disk Groups](#)
- [Dropping Disks from Disk Groups](#)
- [Bringing Disks Online and Offline](#)
- [Dropping Disk Groups](#)
- [Monitoring Disk Group Usage](#)
- [Mounting and Dismounting Disk Groups](#)
- [Administering Advanced Disk Group Properties](#)
- [Specifying a Power Limit For Disk Online](#)
- [Replacing An Existing Disk With a New Disk](#)
- [Setting and Modifying Content Type for the Disk Group](#)
- [Setting and Modifying the Failure Group Repair Time](#)
- [Running Rebalance on Multiple Disk Groups](#)
- [Viewing Rebalance Process Related Data](#)
- [Setting and Modifying the Thin Provisioned Disk Group Attribute](#)
- [Running the On Demand Scrubbing Process](#)
- [Determining Whether Scrubbing Process Is Running](#)

For more information about managing Oracle ASM disk groups, refer to [Administering Oracle ASM Disk Groups](#)

Creating Disk Groups

You can create additional Oracle ASM disk groups to:

- Have disk groups with different redundancy levels (normal, high, or external), depending on availability requirements and storage system capabilities.
- Separate different classes of storage, such as SCSI drives and SATA drives, into different disk groups. Disks in a disk group should have similar size and performance characteristics.
- Store the fast recovery area in a separate disk group from the database.

To create a disk group:

1. Access the Oracle Automatic Storage Management home page.
See "[Accessing the Oracle Automatic Storage Management Home Page](#)" for instructions.
2. Click the **Disk Groups** link at the top of the page to display the Disk Groups property page.
3. If you are not logged in, then the Log In page appears and you should log in as the SYS user, connecting as SYSASM. Provide the SYS password for the Oracle ASM instance. This password was set up when the Oracle ASM instance was created.
4. Click **Create** and Oracle Enterprise Manager displays a Create Disk Group page similar to the page in [Figure 4](#). The Create Disk Group page displays a list of Oracle ASM disks that are available to be added to a disk group. This includes disks with a header status of CANDIDATE, PROVISIONED, or FORMER, and so on.

Figure 4 Oracle Automatic Storage Management Create Disk Group Page

Create Disk Group

* Name

Redundancy: HIGH NORMAL EXTERNAL

Allocation Unit (MB)

An allocation unit (AU) is the fundamental unit in which contiguous disk space is allocated to ASM files. ASM file extent size is a multiple of AUs. The AU size cannot be modified later.

Candidate Member Disks

Select Member Disks:

Select	Path	Header Status	Library	Label	ASM Disk Name	Size	Unit	Force Reuse	Failure Group	Quorum
<input checked="" type="checkbox"/>	/devices/disk1	CANDIDATE	SYSTEM		<input type="text"/>	1024	MB	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	/devices/disk2	CANDIDATE	SYSTEM		<input type="text"/>	1024	MB	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	/devices/disk3	CANDIDATE	SYSTEM		<input type="text"/>	1024	MB	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	/devices/diskm1	CANDIDATE	SYSTEM		<input type="text"/>	1024	MB	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	/devices/diskm2	CANDIDATE	SYSTEM		<input type="text"/>	1024	MB	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	/devices/diskm3	CANDIDATE	SYSTEM		<input type="text"/>	1024	MB	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>

TIP Quorum failure groups are used to store voting files in extended clusters and do not contain any user data. It requires ASM compatibility of 11.2 or higher.

Disk Group Compatibility

Higher compatibility enables the user to use new features available in the newer version. Once the disk group is created, the compatibility version can not be lowered.

Database Compatibility
The minimum software version required for a database instance to use files in this disk group (10.1 and above).

ASM Compatibility
The minimum software version required for an ASM instance to mount this disk group (10.1 and above).

ASM Volume Compatibility
The minimum software version required for an ASM Volume to use this disk group (11.2 and above).

TIP The database compatibility has to be less than or equal to the ASM compatibility. The ASM Volume compatibility can only be set when ASM compatibility is 11.2 and above.

- To display not only disks that are available to be added to a disk group, but all Oracle ASM disks, including disks that belong to a disk group (header status = MEMBER), select **All Disks** from the Select Member Disks list.

The page is re-displayed with the complete list of Oracle ASM disks that were discovered by the Oracle ASM instance.

- Enter the disk name, select a redundancy type (high, normal, or external), and optionally, you can enter a failure group name.
- Select disks as follows:
 - Select the box to the left of each disk to be included in the new disk group.
 - Optionally, you can enter a disk name, the size of the disk for Oracle ASM to use, and the failure group name.
 - To force the inclusion of a disk in the disk group, select the **Force Usage** box for that disk.

Caution:

Selecting the Force Usage box causes the disk to be added to the new disk group even if the disk belongs to another disk group and has valid database data. The existing data is then lost. You must be certain that you are selecting a disk that can legitimately be added to the disk group. See [“Creating Disk Groups”](#) for a discussion of the FORCE option.

8. Specify a **Disk Compatibility** value for the disk group to enable your system to use the latest Oracle ASM features. See [“Configuring Disk Group Compatibility Attributes”](#).
-
-

Note:

You cannot reverse the setting of a disk group compatibility value.

For information about disk group compatibility attributes, see [“Disk Group Compatibility”](#).

9. Click **OK** to create the disk group or click **Cancel** to stop the disk group creation operation. You can also click **Show SQL** to show the SQL statements that the disk group creation operation uses.

For more information about creating disk groups, see [“Creating Disk Groups”](#).

Adding Disks to Disk Groups

You can add disks to a disk group to increase the storage space in a disk group. If you add multiple disks in a single operation, then Oracle ASM rebalances the disk group to evenly distribute the data on all disks, including the newly added disks.

You can control the power of a rebalance operation with the setting of the Rebalance Power. The higher the number, the faster the rebalance operation completes. Lower numbers cause rebalancing to take longer, but consume fewer processing and I/O resources. This leaves these resources available for the database. The default value of 1 minimizes disruption to the database.

A value of 0 blocks the rebalance operation. Manual or automatic rebalance can then occur later. You might want to postpone rebalancing until there are fewer demands on the database, or when you have completed all of your disk group changes.

For information about controlling rebalance operations, refer to [“Manually Rebalancing Disk Groups”](#) and [“Tuning Rebalance Operations”](#). For information about rebalance power settings and the ASM_POWER_LIMIT initialization parameter, refer to [“ASM_POWER_LIMIT”](#).

To add one or more disks to a disk group:

1. Access the Oracle Automatic Storage Management home page.

For instructions, refer to [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click the **Disk Groups** link to display the Disk Groups property page.

3. If the Oracle ASM Login page appears, then log in as the SYS user, connecting as SYSASM. Provide the SYS password for the Oracle ASM instance. This password was set up when the Oracle ASM instance was created.
4. Click a link in the **Name** column to select the disk group to which you want to add disks. The Disk Group page similar to the page in [Figure 6](#) appears, displaying a list of disks that are in the disk group.
5. Click **Add** and Oracle Enterprise Manager displays the Add Disks page. This page displays a list of Oracle ASM disks that are available to be added to the disk group. This includes disks with the header status of CANDIDATE, PROVISIONED, or FORMER, and so on.
6. To display not only disks that are available to be added to a disk group, but all of the Oracle ASM disks, including disks that belong to a disk group (header status = MEMBER), select **All Disks** from the Select Member Disks drop-down list on the right hand side of the page. Oracle Enterprise Manager re-displays the page with the complete list of Oracle ASM disks that were discovered by the Oracle ASM instance.
7. Optionally change the rebalance power by selecting a value from the Rebalance Power list.
8. Select disks as follows:
 - Check the box to the left of each disk to be added to the disk group.
 - To force the inclusion of a disk in the disk group, select the **Force Reuse** box in the right-most column.

Caution:

The Force Reuse box causes the disk to be added to the disk group even if the disk belongs to another disk group and has valid database data. The existing data is then lost. You must be certain that you are selecting a disk that can legitimately be added to the disk group. Refer to [“Adding Disks to a Disk Group”](#) for an example of the FORCE option.

- Optionally enter an Oracle ASM disk name for each disk. Oracle ASM provides a name if you do not.
9. Click **OK** to add the selected disks.

For more information about modifying disk group properties, see [“Altering Disk Groups”](#).

Bringing Disks Online and Offline

Perform the following procedures to bring a disk online or offline:

1. Access the Oracle Automatic Storage Management home page.
See [“Accessing the Oracle Automatic Storage Management Home Page”](#) for instructions.
2. Click the **Disk Groups** link at the top of the page to view the Disk Groups page. Oracle Enterprise Manager displays a page similar to the one shown in [Figure 5](#).

Figure 5 Oracle Automatic Storage Management Disk Groups List Page

Disk Groups

Home Performance **Disk Groups** Configuration Users ASM Cluster File System

Create Mount All Dismount All

Mount Dismount Rebalance Check Scrub Delete

Select All | Select None

Select	Name ▲	State	Redundancy	Size (GB)	Used (GB)	Used (%)	Usable Free (GB)	Member Disks
<input type="checkbox"/>	DATA	MOUNTED	NORMAL	18.00	10.39	57.74	3.30	18
<input type="checkbox"/>	DATA_EXAMPLE	MOUNTED	NORMAL	3.00	0.89	29.56	0.56	3
<input type="checkbox"/>	FRA	MOUNTED	NORMAL	12.00	0.57	4.71	5.22	12

TIP The usable free space specifies the amount of space that can be safely used for data. A value above zero means that redundancy can be properly restored after a disk failure.

TIP Mount All and Dismount All operation will only mount and dismount the disk groups specified in the Auto Mount Disk Groups parameter.

- Click the name of a disk in the Name column and Oracle Enterprise Manager displays the General page for the disk group to modify. The General page that you see should be similar to the one shown in Figure 6 .

Figure 6 Oracle Automatic Storage Management Disk Group General Page

Disk Group: DATA

General Performance Templates Files Access Control Volumes

General

Name: DATA
 State: MOUNTED
 Redundancy: NORMAL
 Total Size (GB): 18
 Pending Operations: 0
 Allocation Unit (MB): 1

Advanced Attributes

Database Compatibility: 12.1.0.0.0
 ASM Compatibility: 12.1.0.0.0
 ASM Volume Compatibility: 12.1.0.0.0
 Disk Repair Time (Hours): 3.6
 Smart Scan Capability: Disabled
 File Access Control: Disabled
 Failure Group Repair Time (Hours): 24.0
 Disk Group Content: Data
 Thin Provisioned: Disabled
 Content Checking: Disabled

Current Disk Group Usage (GB)

Free(7.61) 42%
 System(0.34) 2%
 ASM(0.00) 0%
 ORCL(6.05) 34%
 ACFS 11%
 Volumes(2.00) 11%
 Other 11%
 Volumes(2.00)

Disk Group Daily Space

No data is c

Member Disks

View: By Disk Go Add

Resize Online Offline Recover Bad Blocks Replace Scrub Remove

Select All | Select None

Select	Disk ▲	Failure Group	Path	Library	Read/Write Errors	State	Mode	Size (GB)	Used (GB)	Used (%)	Failgroup Type
<input type="checkbox"/>	DATA_0000	DATA_0000	/devices/diska1	SYSTEM	0	NORMAL	✓	1.00	0.60	60.25	REGULAR

- To bring a disk online, select the disk to bring online and click **Online**. If you bring a disk online, then Oracle ASM performs the following:
 - Oracle ASM performs the online operation on the selected disks. You can select one or more or disks, or all of the disks to bring online. If you select all of the disks, then Oracle uses the ALL keyword for this operation. Otherwise, only the selected disks are affected by the online operation.

- During the online process, Oracle Enterprise Manager first places a disk into online mode to accommodate write operations. Then Oracle Enterprise Manager resynchronizes stale data on the disk with the current data until the disk is fully online for read operations; this is the Oracle ASM fast mirror resync feature.
 - You can also choose the By Failure Group view to perform this operation on a selected disk group. In this case, Oracle uses the SQL for disks in failure group.
 - You can also select a disk that is online, but Oracle Enterprise Manager ignores that selection and only brings disks online that were previously offline.
 - Click **Yes** on the Oracle Enterprise Manager Confirmation dialog to begin bringing the disk online or click **No** to cancel the operation. You can also click **Show SQL** to review the SQL that Oracle Enterprise Manager uses for the online operation.
5. To take a disk offline, select the disk to take offline and click **Offline**. If you bring a disk offline, then Oracle ASM performs the following:
- Depending on how much data is stale, the operation may require additional time to complete. You can monitor the operation's progress using the Pending Operations link from the Disk Group home page.
 - The value that you set for Rebalance Power using `ASM_POWER_LIMIT` must be a whole number. The text on the page describes how the value of Rebalance Power affects the fast mirror resync operation. If the `ASM_POWER_LIMIT` is set to 0, then Oracle ASM does not perform automatic rebalance. For information about rebalance power settings and the `ASM_POWER_LIMIT` initialization parameter, refer to "[ASM_POWER_LIMIT](#)".
 - By default, the Rebalance Power value uses the value of the `ASM_POWER_LIMIT` initialization parameter.
 - Oracle Enterprise Manager displays an Offline Confirmation page and the text on this page explains that after Oracle Enterprise Manager takes the selected disks offline, the Oracle ASM instance waits for the time interval that is specified by the value that you have set for the `DISK_REPAIR_TIME` initialization parameter before Oracle ASM drops the disks. During the disk repair time period, you can repair the disks and then place them back online. For each disk that you successfully place online, the pending drop operation is canceled and a resynchronization operation begins.
 - If you have set `DISK_REPAIR_TIME` to a large value, for example, greater than one day, then this increases the possibility of data loss. This is because the files in the disk group are protected with a lower degree of redundancy during this period.
- Click **Yes** on the Oracle Enterprise Manager Confirmation dialog to begin the offline processing or click **No** to stop the operation. You can also click **Show SQL** to see the SQL that Oracle Enterprise Manager uses for the offline operation.

Dropping Disks from Disk Groups

When you drop a disk from a disk group, Oracle ASM rebalances the disk group by moving all of the file extents from the dropped disk to other disks in the disk group.

Oracle ASM then releases the disk and you can then add the disk to another disk group or use it for other purposes. You can drop one or more disks in a single operation. You can also optionally set rebalance power for the drop operation. The following is a list of possible reasons for dropping a disk:

- A disk is starting to fail and you must replace it
- To upgrade a disk
- To reallocate the disk to a different disk group or reallocate the disk to a different storage system

Note:

Dropping disks from a disk group only logically deletes the disks from the disk group. It does not delete the disk contents. However, the contents are lost when you add the disk to a new disk group.

To drop one or more disks from a disk group:

1. Access the Oracle Automatic Storage Management home page.
See "[Accessing the Oracle Automatic Storage Management Home Page](#)" for instructions.
2. Click the **Disk Groups** link to display the Disk Groups property page.
3. If the Oracle Automatic Storage Management Login page appears, log in as the SYS user, connecting as SYSASM. Provide the SYS password for the Oracle ASM instance. This password was set up when the Oracle ASM instance was created.
4. Click a link in the **Name** column to select the disk group that contains the disks to be dropped.
The Disk Group page appears.
5. Under the Member Disks heading, in the Select column, select the boxes for the disks that you plan to drop, and then click **Remove**.
A confirmation page appears.
6. To change the rebalance power, or to set the FORCE option for dropping disks, do the following:
 - a. Click **Show Advanced Options**.
 - b. Optionally select the **Force** option or select a rebalance power in the **Rebalance Power** list.

Note:

You might need the FORCE option if Oracle ASM cannot read from or write to the disk. For a discussion of the FORCE option, see "[Dropping Disks from Disk Groups](#)".

7. Click **Yes** to drop the disks.

The **Disk Group** page returns, and displays a state of `DROPPING` for each disk being dropped.

8. Refresh the page until the dropped disks no longer appear in the disk group.

Caution:

You cannot reuse or disconnect the dropped disks until the drop and rebalance operations are complete. Operations are complete when the dropped disks no longer appear in the disk group. For more information about dropping disks, see [“Dropping Disks from Disk Groups”](#).

Dropping Disk Groups

When you drop a disk group, you delete the disk group optionally with all of its files. You cannot drop a disk group if any of its database files are open. Oracle ASM deletes all of the disk group contents only if you specify the **including contents** option. After dropping a disk group, you can add its member disks to other disk groups or use them for other purposes.

One reason to drop a disk group is to change the redundancy level (normal, high, or external). Because you cannot change the redundancy of a disk group, you must drop the disk group and then re-create it with the proper redundancy. In this case, you must back up or move disk group data before you drop the disk group.

To drop a disk group:

1. Access the Oracle ASM home page.
See [“Accessing the Oracle Automatic Storage Management Home Page”](#) for instructions.
2. Click the **Disk Group** tab to display the Disk Groups page.
3. If the Oracle ASM Login page appears, log in as the `SYS` user, connecting as `SYSASM`. Provide the `SYS` password for the Oracle ASM instance. This password was set up when the Oracle ASM instance was created.
4. Click the box in the **Select** column to select a disk group that you plan to drop.
5. Click **Delete** and the confirmation page appears.
6. To delete the disk group even if it still contains files, click **Show Advanced Options** and ensure that the **Including Contents** option is selected. If the disk group contains files and the **Including Contents** option is not selected, then you cannot drop the disk group.
7. To delete a disk group that belongs to a disk group that you cannot mount, use the `FORCE` option in the Advanced Options confirmation dialog. The `FORCE` option applies to the `DISMOUNTED` disk group only. This option enables you to delete a disk header and mark it as `FORMER`.

Caution:

Use extreme care when using the `FORCE` option because the Oracle ASM instance does not verify whether the disk group is used by any other Oracle ASM instance before Oracle ASM deletes the disk group.

8. On the confirmation page, click **Yes**.

For more information about dropping disks, see [“Dropping Disk Groups”](#).

Monitoring Disk Group Usage

Perform the following procedures to monitor disk group usage:

To view Oracle ASM disk group usage and free space:

1. Access the Oracle Automatic Storage Management home page.
See [“Accessing the Oracle Automatic Storage Management Home Page”](#) for instructions.
2. Click the **Disk Groups** link to view the Disk Groups property page.
3. If the Oracle ASM Login page appears, then log in as the `SYS` user, connecting as `SYSASM`. Provide the `SYS` password that was set up for Oracle ASM when the Oracle ASM instance was created.

The Disk Group list page, similar to the page shown in [Figure 5](#), displays all of the disk groups and their space usage information.

The Usable Free column displays the space in megabytes that is available in the disk group. The values in this column consider the redundancy level of the disk group, and exclude the space that the disk group reserves for restoring full redundancy for all files in the disk group after a disk failure.

For more information, see [“Managing Capacity in Disk Groups”](#) and [“Views Containing Oracle ASM Disk Group Information”](#)

Mounting and Dismounting Disk Groups

Use the `FORCE` option to mount a disk group when there are missing disks or missing failure groups. The `FORCE` option corrects configuration errors, such as incorrect values for `ASM_DISKSTRING`, without incurring unnecessary rebalance operations. Disk groups mounted with the `FORCE` option have one or more disks offline if the disks were not available at the time of the mount. You must take corrective action to restore those devices before the time set with the `DISK_REPAIR_TIME` value expires. Failing to restore and put those disks back online within the disk repair time frame results in Oracle ASM automatically removing the disks from the disk group. This would then require a rebalance operation to restore redundancy for all of the files in the disk group. Perform the following procedures to mount a disk with the `FORCE` option:

1. From the Oracle ASM home page click the **Disk Groups** tab.
2. Select the disk group that has a disk that you must repair and click **Dismount**. Click **OK** on the Dismount confirmation dialog. The State column of the Disk Group home page should show the Status as `DISMOUNTED`.
3. Perform any needed repairs to the disk in the disk group.

4. Click the box in the Select column next to the disk that you plan to force mount, then click **Mount**.
5. On the Disk Mount Confirmation dialog, click the **Show Advanced Options** link.
6. On the Mount Force Confirmation dialog, select the **Force** option and click **Yes**. You can also click **No** to cancel the mount force operation and **Show SQL** to review the SQL that Oracle Enterprise Manager uses to perform the mount force operation.

Administering Advanced Disk Group Properties

This section explains how to administer advanced disk group properties.

Perform the following steps to change the values for disk group attributes that can be altered after the disk group has been created.

1. On the Automatic Storage Disk Group List page, click a disk group name and Oracle Enterprise Manager displays the Disk Group home page.
2. Click **Edit** under the Advanced Attributes section.

The topics contained in this section are:

- [Configuring Disk Group Compatibility Attributes](#)
- [Configuring Disk Repair Time](#)
- [Configuring Smart Scan Compatibility](#)
- [Configuring File Access Control](#)

Figure 7 shows the advanced attributes that can be altered for an existing disk group. This screenshot only shows the top portion of the **Edit Advanced Attributes for Disk Group** Page.

Figure 7 Oracle Automatic Storage Management Edit Advanced Attributes Page

Edit Advanced Attributes for Disk Group: DATA Show SQL Cancel OK


Disk Group Compatibility

Advancing the disk group compatibility enables the user to use new features available in the newer version. This operation can not be reversed.

Database Compatibility
The minimum software version required for a database instance to use files in this disk group (10.1 and above).

ASM Compatibility
The minimum software version required for an ASM instance to mount this disk group (10.1 and above).

ASM Volume Compatibility
The minimum software version required for an ASM Volume to use this disk group (11.2 and above).


 **TIP** The database compatibility has to be less than or equal to the ASM compatibility. The ASM Volume compatibility can only be set when ASM compatibility is 11.2 and above.

Repair Time

Specify a time period that is long enough for you to repair the disk/failure group. Failure group repair time should be greater than Disk repair time and note that larger the values

Failure Group Repair Time Hours
The failure Group Repair Time applies to all the failure groups in the Disk Group except those containing only one Disk. This value will override the

Disk Repair Time Hours
Disks will be dropped after the specified time has passed.

 **TIP** Disk repair time and Failure group repair time attribute can be set only if the ASM compatibility is greater than or equal to 11.1.0.0 and 12.1.0.0 respectively and diskgroup

Configuring Disk Group Compatibility Attributes

Specify a **Disk Compatibility** value for the disk group to enable your system to use the latest Oracle ASM features.

Note:

You cannot reverse the setting of a disk group compatibility value.

- **ASM Compatibility**

Specify the value that is the minimum software version required for an Oracle ASM instance to mount this disk group.

- **Database Compatibility**

Specify a value that must be less than or equal to the Oracle ASM compatibility. This is the minimum software version that is required for a database instance to use the files in the disk group. If the database compatibility value that you use is greater than the Oracle ASM compatibility, then Oracle Enterprise Manager displays an error.

Note:

You cannot modify the database compatibility for an Oracle ASM cluster that is in a rolling migration state.

- **ASM Volume**

Specify a value that is 11.2 or greater to use the Oracle ASM Dynamic Volume Manager (Oracle ADVM) functionality. The ASM compatibility of the disk group must be set to 11.2 or greater to enable Oracle ADVM. Also, the Oracle ADVM volume drivers must be loaded in the supported environment.

For information about disk group compatibility attributes, see [“Disk Group Compatibility”](#).

Configuring Disk Repair Time

Specify a time period that is long enough for you to repair a disk in the disk group.

For information about disk group repair time, see [“Oracle ASM Fast Mirror Resync”](#).

Configuring Smart Scan Compatibility

Specify to disable or enable smart scan compatibility for the disk group.

This attribute is only applicable to Oracle Exadata storage.

See Also:

Oracle Exadata documentation for information about the `CELL.SMART_SCAN_CAPABLE` attribute

Configuring File Access Control

Specify to disable or enable Oracle ASM File Access Control. If Oracle ASM File Access Control is enabled, then specify the default permissions for newly created files in the disk group.

For information about Oracle ASM File Access Control, see [“Managing Oracle ASM File Access Control for Disk Groups”](#).

Specifying a Power Limit For Disk Online

To specify a power limit for disk online, follow these steps:

1. Access the Oracle Automatic Storage Management home page.
See [“Accessing the Oracle Automatic Storage Management Home Page”](#) for instructions.
2. Select the **Disk Groups** tab. The Disk Groups page is displayed.
3. Select a disk group. The Disk Group page appears and shows all Member Disks that belong to the disk group in the Member Disks table.
4. Select a disk, then click **Online**. The online confirmation page is displayed with the advance option to specify a power limit.
5. Specify the **Power Limit**, then click **Submit**. The disk is set to online with the specified power limit.

For information about the power option in rebalancing a disk group, refer to [“Manually Rebalancing Disk Groups”](#). For information about the `ASM_POWER_LIMIT` initialization parameter, refer to [“ASM_POWER_LIMIT”](#).

Replacing An Existing Disk With a New Disk

To replace an existing disk with a new disk, follow these steps:

1. Access the Oracle Automatic Storage Management home page.
See [“Accessing the Oracle Automatic Storage Management Home Page”](#) for instructions.
2. Click the Disk Group tab. The Disk Group page displays.
3. Select a Disk Group. The Disk Group page appears which shows all Member Disks that belong to the disk group.
4. Select an offline disk to replace. The Replace Disks page is displayed.
Select a new disk of size equal to or greater than the original disk being replaced to ensure the same level of data protection.
5. Select a new disk and then specify the options, such as Rebalance Power, and then click **OK**. The disk is then replaced. Rebalance operations redistribute data evenly across all drives. Oracle ASM automatically rebalances a disk group whenever disks are added or dropped. To manually rebalance all disk groups, you must specify the Rebalance Power. Higher values use more I/O bandwidth and complete rebalance more quickly. Lower values cause rebalance to take longer, but use less I/O bandwidth. Values range from 0 to 1024.

For additional information about replacing a disk, refer to [“Replacing Disks in Disk Groups”](#).

Setting and Modifying Content Type for the Disk Group

To set and modify the content type for a disk group, follow these steps:

1. Access the Oracle Automatic Storage Management home page.

See [“Accessing the Oracle Automatic Storage Management Home Page”](#) for instructions.
2. Click the Disk Groups tab. The Disk Group page displays.
3. Click **Create**. In the Disk Resync Attributes section of the Create Disk Group page, you can select the value **Recovery**, **Data** or **System** from the **Content Type** drop-down list. The attribute can be set only if the ASM compatibility is greater than or equal to 12.1.0.0.
4. To edit the content type for an existing disk group, navigate to the Disk Group home page by clicking the disk group in the Disk Groups table. The Disk Group home page displays.
5. Click **Edit** in the Advanced Attribute Section. The Edit Advanced Attributes for Disk Group page appears. In the Disk Resync Attributes section, select from the values **Recovery**, **Data**, or **System** from the **Content Type** drop-down list.

For information about the `CONTENT.TYPE` disk group attribute, refer to [“CONTENT.TYPE”](#).

Setting and Modifying the Failure Group Repair Time

To set and modify the Failure Group Repair Time, follow these steps:

1. Access the Oracle Automatic Storage Management home page.

See [“Accessing the Oracle Automatic Storage Management Home Page”](#) for instructions.
2. Click the Disk Groups tab. The Disk Groups page displays.
3. Click **Create**. Specify the repair time for the **Failure Group** in the Candidate Member Disks table.
4. To edit an existing Failure Group repair time, from the Disk Group page choose the **Disk Group** for the repair time you want to modify. The Disk Group page appears.
5. In the Advanced Attributes section, click **Edit**. The Edit Advanced Attributes for Disk Group page displays.
6. In the Disk Resync Attributes section, modify the **Failure Group Repair Time**, then click **OK**. The failure Group Repair Time applies to all the failure groups in the disk group except those containing only one disk. This value overrides the disk repair time and is overridden by the actual value provided when a disk is taken offline.

For additional information about setting and modifying the failure group repair time, refer to [“Oracle ASM Fast Mirror Resync”](#).

Running Rebalance on Multiple Disk Groups

Enterprise Manager enables you to rebalance on multiple disk groups and distribute the data copy across other member instances in the cluster. To run rebalance on multiple disk groups, follow these steps:

1. Access the Oracle Automatic Storage Management home page.

See “[Accessing the Oracle Automatic Storage Management Home Page](#)” for instructions.
2. Click the Disk Group tab. The Disk Group page displays.
3. Select multiple disk groups then click **Rebalance**. The Rebalance Disk Groups Confirmation page appears where you can set the Rebalance Power by displaying Advanced Options.
4. Set the Rebalance Power value, then click **OK**. The command to rebalance is submitted.

For additional information about rebalancing disk groups, refer to “[Manually Rebalancing Disk Groups](#)”.

Viewing Rebalance Process Related Data

To view rebalance process-related data, including the number of participating instances on the Pending Operations page, follow these steps:

1. Access the Oracle Automatic Storage Management home page.

See “[Accessing the Oracle Automatic Storage Management Home Page](#)” for instructions.
2. Click the Disk Group tab. The Disk Groups page displays.
3. Click a Disk Group link. The Disk Group home page General section displays the number of **Pending Operations** as a link to the Pending Operations page.
4. Click the link. Information on the rebalance process, along with details on the number of participating instances, are displayed.

For additional information about rebalancing disk groups, refer to “[Tuning Rebalance Operations](#)”.

Setting and Modifying the Thin Provisioned Disk Group Attribute

To set and modify the thin-provisioned disk group attribute, follow these steps:

1. Access the Oracle Automatic Storage Management home page.

See “[Accessing the Oracle Automatic Storage Management Home Page](#)” for instructions.
2. Click the Disk Groups tab. The Disk Groups page is displayed.
3. Click the Disk Group that contains the Thin Provisioned attribute you want to change. The Disk Group page displays.

4. In the Advance Attributes section, click **Edit**. The Edit Advanced Attributes for Disk Group page displays.
5. In the Thin Provisioning section, select **True** or **False** from the Thin Provisioned field drop-down list. If thin provisioning is enabled, the disk space not in use can be returned to the array. This attribute can be set only if the ASM compatibility is greater than or equal to 12.1.0.0.

For information about the THIN_PROVISIONED disk group attribute, refer to [“THIN_PROVISIONED”](#).

Running the On Demand Scrubbing Process

To run the On Demand scrubbing process, follow these steps:

1. Access the Oracle Automatic Storage Management home page.
See [“Accessing the Oracle Automatic Storage Management Home Page”](#) for instructions.
2. Click the Disk Group tab. The Disk Group page is displayed.
3. Click **Scrub**. The Scrub Disk Group page is displayed where you can use advanced options such as repair, power level, wait and force. You can also use the scrub action on disks and files.
4. Provide the advance option and click **OK**. A background process is initiated that scrubs the disk group.

For additional information about scrubbing disk groups, refer to [“Scrubbing Disk Groups”](#).

Determining Whether Scrubbing Process Is Running

To determine whether the scrubbing process is running, follow these steps:

1. Access the Oracle Automatic Storage Management home page.
See [“Accessing the Oracle Automatic Storage Management Home Page”](#) for instructions.
2. Click the Disk Group tab. The Disk Group page displays.
3. Click a Disk Group link. The Disk Group General Section displays a Pending Operation link if a scrubbing process is ongoing.
4. Click the link. Details on the scrubbing process are displayed.

Managing Oracle ASM File Access Control with Oracle Enterprise Manager

You can manage Oracle ASM File Access Control with Oracle Enterprise Manager Integration for Oracle ASM File Access Control, shown in [Figure 8](#).

Figure 8 Oracle Automatic Storage Management Disk Group Access Control Home Page

Disk Group: DATA

General Performance Templates Files **Access Control** Volumes

Users

In order to have access to files on a disk group, operating system users need to be granted access privileges to the disk group. Once granted access privileges, users can be added to the disk group.

Current Users: None

Add Replace Remove

Groups

A group contains a list of operating system users. File access privileges can be granted to the group. Members of the group inherit the file access privileges granted to the group.

Create

Select	Name	Owner	Members	Edit
	No items found			

To manage Oracle ASM File Access Control:

1. Access the Oracle Automatic Storage Management home page.
See "[Accessing the Oracle Automatic Storage Management Home Page](#)" for instructions.
2. Click the **Disk Groups** link to display the Disk Groups property page.
3. Click a link in the **Name** column to select a disk group.
4. Click the **Access Control** tab to display the **Access Control** page.

On this page, you can add, remove, or replace users from a user group and create or delete user groups. You can also modify the ownership or permission of files.

To access files in a disk group, operating system users must be granted access privileges to the disk group. After granted access privileges, users can be added as members of groups. The operating system user who owns the oracle binary for the database instance is automatically added and cannot be removed.

Oracle ASM File Access Control operations on this page are available when the files are open.

For more information about Oracle ASM File Access Control, see "[Managing Oracle ASM File Access Control for Disk Groups](#)".

Managing Directories, Files, and Aliases with Oracle Enterprise Manager

You can manage directories, files, and aliases with the **Files** tab of the Oracle Enterprise Manager Disk Group page, shown in [Figure 9](#).

Figure 9 Oracle Automatic Storage Management Files Tab

Disk Group: DATA

General Performance Templates **Files** Access Control Volumes

The following are the directories, files and aliases associated with the serviced databases in this disk group.

Create Alias Create Directory Rename Edit File Scrub Delete

Select All | Select None | Expand All | Collapse All

Select	Name	Physical Size (KB)	Logical Size (KB)	Primary Region	Mirror Region	Permissions			Ownership	
						Owner	Group	Other	Owner	Group
<input type="checkbox"/>	DATA									
<input type="checkbox"/>	ASM									
<input type="checkbox"/>	ASMPARAMETERFILE									
<input type="checkbox"/>	PASSWORD									
<input type="checkbox"/>	ORCL									
<input type="checkbox"/>	CONTROLFILE									
<input type="checkbox"/>	DATAFILE									
<input type="checkbox"/>	SYSAUX.257.803831781	4019200	2007048	COLD	COLD	Read-write	Read-write	Read-write		
<input type="checkbox"/>	SYSTEM.258.803831845	1664000	829448	COLD	COLD	Read-write	Read-write	Read-write		
<input type="checkbox"/>	UNDOTBS1.260.803831901	138240	66568	COLD	COLD	Read-write	Read-write	Read-write		
<input type="checkbox"/>	USERS.259.803831901	12288	5128	COLD	COLD	Read-write	Read-write	Read-write		

To manage Oracle ASM files:

1. Access the Oracle Automatic Storage Management home page.
See “[Accessing the Oracle Automatic Storage Management Home Page](#)” for instructions.
2. Click the **Disk Groups** link to display the Disk Groups property page.
3. Click a link in the **Name** column to select a disk group.
4. Click the **Files** tab to display the **Files** page.
5. Click the icons to left on the folders to expand or contract the folders. When you expand the folders, you can drill down to individual files.
6. You can select a file with the **Select** box, then click **Rename** to rename the file, click **Edit** to change the properties of a file, or click **Delete** to remove a file. You can click the name of a file to display the properties page.

For more information about managing Oracle ASM files, directories, and aliases, see [Administering Oracle ASM Files_ Directories_ and Templates](#).

Managing Disk Group Templates with Oracle Enterprise Manager

You can manage disk group templates with the Templates tab of the Disk Group page, shown in [Figure 10](#).

Figure 10 Oracle Automatic Storage Management Templates Page

Disk Group: DATA

General Performance **Templates** Files Access Control Volumes

Create

Edit Delete

Select	Name	Redundancy	Striped	System	Primary Region	Mirror Region
<input checked="" type="radio"/>	PARAMETERFILE	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	OCRFILE	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	VOTINGFILE	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	DUMPSET	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	CONTROLFILE	High	Fine	Yes	COLD	COLD
<input type="radio"/>	FLASHFILE	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	ARCHIVELOG	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	ONLINELOG	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	DATAFILE	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	TEMPFILE	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	BACKUPSET	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	XTRANSPORT BACKUPSET	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	INCR XTRANSPORT BACKUPSET	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	AUTOBACKUP	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	XTRANSPORT	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	CHANGETRACKING	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	FLASHBACK	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	KEY_STORE	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	AUTOLOGIN_KEY_STORE	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	AUDIT_SPILLFILES	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	DATAGUARDCONFIG	Mirror	Coarse	Yes	COLD	COLD
<input type="radio"/>	ASMPARAMETERFILE	Mirror	Coarse	Yes	COLD	COLD

Edit Delete

To manage Oracle ASM templates:

1. Access the Oracle Automatic Storage Management home page.
See “[Accessing the Oracle Automatic Storage Management Home Page](#)” for instructions.
2. Click the **Disk Groups** link to display the Disk Groups property page.
3. Click a link in the **Name** column to select a disk group.
4. Click the **Templates** tab to display the Templates page.
5. You can click **Create** to add a new template, click **Edit** to change a page, or click **Delete** to remove a template.

If you click **Create**, then the Create Template page displays and you can enter a name in the Template Name field. You can also specify a redundancy level, striped granularity, and extent regions (hot or cold).

For more information about disk group templates, see “[Managing Disk Group Templates](#)”. For information about hot and cold disk regions, see “[Intelligent Data Placement](#)”.

Managing Oracle ASM Filter Driver With Oracle Enterprise Manager

You can manage Oracle ASM Filter Driver with Oracle Enterprise Manager.

This section contains the following sections:

- [Discovering ASM Filter Driver Disks](#)
- [Provisioning ASM Filter Driver Disks](#)
- [Releasing ASM Filter Driver Disks](#)

For more information about managing Oracle ASM Filter Driver, refer to “[Oracle ASM Filter Driver](#)”.

Discovering ASM Filter Driver Disks

To discover disks for Oracle ASM Filter Driver follow these steps:

1. From **Targets** menu, select **All Targets**.
2. On the All Targets page, select any target of type **Automatic Storage Management**.
3. On the target home page, from **Automatic Storage Management** menu, select **Configuration Parameters**.
4. On the Configuration page, click **Manage Disk Provisioning**. The ASM Filter Driver Page is displayed.
5. On the Disks available for Provisioning table, click **Discover** to discover additional Oracle ASM disks.
6. In the Discover Disks dialog box, enter additional discovery paths from where you would like to provision disks. If you are providing more than one path, then ensure that the values are separated by a comma.

For example, ' /dev/ ' , ' /tmp ' .

7. Click **Ok**.

In the Disks available for Provisioning table, all the disks available in the discovery paths are listed.

Provisioning ASM Filter Driver Disks

To provision a set of disks for Oracle ASM Filter Driver, follow these steps:

1. From **Targets** menu, select **All Targets**.
2. On the All Targets page, select any target of type **Automatic Storage Management**.
3. On the target home page, from **Automatic Storage Management** menu, select **Configuration Parameters**.
4. On the Configuration page, click **Manage Disk Provisioning**. The ASM Filter Driver Page is displayed.
5. From the Disks available for Provisioning table, select one or more disks, then click **Provision**.
6. The Provision Disks dialog box lists all the disks that were selected for provisioning. You can update the Label info if you want, then click **OK**.

After provisioning, the Oracle ASM disks appear in the Provisioned Disks table. These disks display with their new label. For example, if you select /dev/loop3 to be

provisioned with a label LOOP3 , then after provisioning the disk displays as AFD:LOOP3 in the Provisioned Disks table.

After the disks are provisioned, they become eligible to be managed by the Oracle ASM Filter Driver.

Releasing ASM Filter Driver Disks

To release the disks currently managed by Oracle ASM Filter Driver, follow these steps:

1. From **Targets** menu, select **All Targets**.
2. On the All Targets page, select any target of type **Automatic Storage Management**.
3. On the target home page, from **Automatic Storage Management** menu, select **Configuration Parameters**.
4. On the Configuration page, click **Manage Disk Provisioning**. The ASM Filter Driver Page is displayed.
5. From the Provisioned Disks table, select one or more disks, then click **Release**.
6. In the Release Provisioned Disks dialog box, click **Yes** to release the disks

After the disks are released, they are removed from the Provisioned Disks table. They instead appear in the Disks available for provisioning table as a candidate eligible to be provisioned.

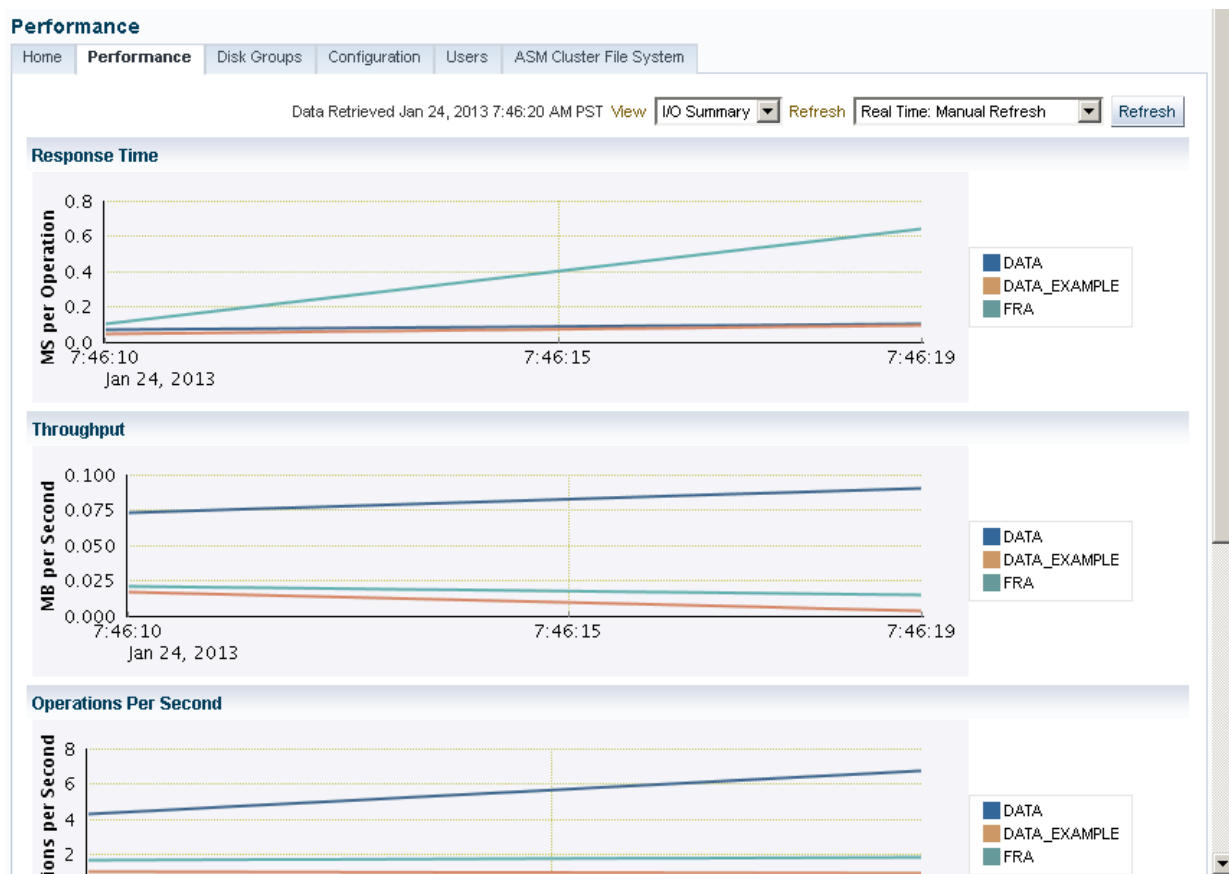
Monitoring Oracle ASM Performance With Oracle Enterprise Manager

This section describes how to perform the following performance-related Oracle ASM administrative tasks:

- [Monitoring General Oracle ASM Performance](#)
- [Checking Disk Group Integrity](#)

Monitoring General Oracle ASM Performance

You can monitor Oracle ASM performance with the Oracle Enterprise Manager Performance page, shown in [Figure 11](#) .

Figure 11 Oracle Automatic Storage Management Performance Page

To monitor Oracle ASM performance:

1. Access the Oracle Automatic Storage Management home page.
See "[Accessing the Oracle Automatic Storage Management Home Page](#)" for instructions.
2. Click the **Performance** link to view the Performance property page.
3. Determine the view and refresh rate of the performance graphs with the **View** and **Refresh** options. Click **Refresh** to manually refresh the graphs. The refresh option has the following two intervals:
 - Manual refresh: manual, 15 second interval, 30 second interval
 - Historical data: Last 24 hours, last 7 days, last 31 days

For more information, refer to "[Performance and Scalability Considerations for Disk Groups](#)".

Checking Disk Group Integrity

When you check the integrity of Oracle ASM disk groups, Oracle Enterprise Manager performs consistency checks on all of the disk group metadata. If Oracle ASM detects errors, then Oracle ASM stores information about errors in the alert log. To check disk groups, perform the following steps:

1. From the **Disk Groups** page, select a disk group in the list and click **Check**.

A confirmation dialog for the check disk group operation displays.

Figure 12 Oracle Automatic Storage Management Check Diskgroup Confirmation Dialog

2. Select **Check Without Repair** to record information about disk group inconsistencies in the alert log. In this operation, Oracle ASM does not resolve the errors. Select **Check And Repair** to attempt to repair errors that Oracle Enterprise Manager identifies during the disk group consistency check.
3. Click **Yes** to start the disk group check operation or **No** to cancel it. You can also select **Show SQL** to review the SQL statements that the disk group check operation uses. Click **OK** to run the check operation as a command. To schedule a job, click **Schedule Job**. Optionally, you can modify or reenter the job name and description. Also provide host credentials and enter the scheduling options by selecting **Immediately** or **Later** and modifying the date and time as needed. Click **OK** to schedule the job or **Cancel** to terminate the job creation process.

Backing Up Oracle ASM Files with Oracle Enterprise Manager

Oracle recommends that you use RMAN to back up files managed by Oracle ASM. The procedures for using RMAN are documented in *Oracle Database 2 Day DBA*.

You can also back up your Oracle ASM managed files by performing a files related operation using the following procedures:

1. Create an alias.
2. Create a directory.
3. Delete the alias and directory.
4. Rename the alias and directory.

For information about migrating data with RMAN, see [Performing Oracle ASM Data Migration with RMAN](#).

See Also:

For additional information about RMAN, refer to the *Oracle Database Backup and Recovery User's Guide*.

Performing Bad Block Recovery with Oracle Enterprise Manager

The procedures that you use in Oracle Enterprise Manager to perform bad block recovery correspond to the steps that you could manually perform with the `remap`

command using the Oracle ASM Command utility (ASMCMD). Use the following procedures to perform bad block recovery:

1. Access the Oracle Automatic Storage Management home page.

See “[Accessing the Oracle Automatic Storage Management Home Page](#)” for instructions.
2. Click the **Disk Groups** link at the top of the page.
3. If you are not logged in, then the Log In page appears and you should log in as the SYS user, connecting as SYSASM. Provide the SYS password for the Oracle ASM instance. This password was set up when the Oracle ASM instance was created.
4. Click a disk group name and Oracle Enterprise Manager displays the disk group home page for that disk group.
5. Click a box in the Select column to the left of a disk in which to recover bad blocks, then click **Recover Bad Blocks**.

Note:

You can only recover bad blocks for disk groups that you have configured with normal or high redundancy; you cannot use this feature for disk groups that you have configured with external redundancy.

Migrating to Oracle ASM with Oracle Enterprise Manager

This section explains how to use Oracle Enterprise Manager to migrate your database storage to use Oracle ASM.

Perform the following steps to migrate to Oracle ASM:

1. At the top of the Oracle Enterprise Manager Database Instance home page, click the **Administration** pull down list and select **Migrate to Oracle ASM**.
2. You may need to set credentials for the database, Oracle ASM, and host.

If prompted for database login credentials, then enter the user `SYS`, provide the `SYS` password that was set for the Oracle Database instance during installation, and connect as `SYSDBA`.

If prompted for Oracle ASM login credentials, then enter the user `SYS`, provide the `SYS` password that was set for the Oracle ASM instance during installation, and connect as `SYSASM`. For more information about authentication, see “[Authentication for Accessing Oracle ASM Instances](#)”.
3. On the **Migrate Database To ASM: Migration Options Page**, which is the first step in a four-step process, verify the information about the files that you plan to migrate to Oracle ASM. If the target database is in `ARCHIVELOG` mode, then you could perform online or offline migration by selecting the corresponding option. Otherwise, using offline migration is the default. If you perform an online migration, then you can suspend the migration by selecting the check box next to **Suspend Migration Job Before Switching Database To ASM**.

Additionally, you can enter an e-mail address to which Oracle Enterprise Manager sends a message to notify you about the suspension. By default on this page, the Recovery-related Files option is selected. Deselect this option if you do not want to

use it. Also verify the entry for the initialization parameter file. Lastly, the **Parallelize File Copy Operations** option is selected by default. Deselect this if you do not want Oracle Enterprise Manager to perform copy operations in parallel. Click **Next** when you complete your selections on this page and Oracle Enterprise Manager displays the **Migrate Database To ASM: Disk Group Options** page.

4. On the Disk Group Options page under Database Area, verify the location where Oracle ASM should create data files, temporary files, redo log files, and control files. Also verify the fast recovery area where Oracle ASM should create the recovery-related files such as archived redo log files, backup files, and so on. Also under fast recovery area, the option for Setup fast recovery area without Migrating Recovery-related Files is selected by default. If needed, change the selection to migrate the files. Click **Next** when you complete your selections on the Disk Group Options page.
5. If you chose to use a fast recovery area and Oracle Enterprise Manager displays a warning that the available space on the disk group is less than the specified fast recovery area size for the migration, then you can either continue by clicking **Yes**, or click **No** to stop the operation and modify your storage.
6. When you continue, Oracle Enterprise Manager displays the Schedule page on which you can specify a job name and a date and time for the migration job to begin. Click **Next** when you have configured your desired settings.
7. Oracle Enterprise Manager displays the Review page on which you can review all of your selections before beginning your migration operation. To expand the tablespace details and review them, click the plus (+) sign next to Tablespaces and Files To Be Migrated. Click **Back** to modify any of your selections or **Submit Job** to begin the migration. Click **Cancel** to cancel the operation.

Note:

If your migration job fails, then do not start your database until you complete a recovery operation. Otherwise, you may corrupt your database.

8. After you submit your job, Oracle Enterprise Manager should display a confirmation dialog indicating that the migration job was successful. Click **View Status** on the confirmation dialog to examine the progress of your migration job.

After the migration job has completed, the Oracle ASM links on the Oracle Enterprise Manager page may not display immediately. You may need to wait for the links to display after a subsequent refresh.

Monitoring Alerts and Incidents With Oracle ASM Support Workbench

Oracle Enterprise Manager provides Support Workbench to monitor Oracle ASM alerts and incidents.

To access Support Workbench, select **Diagnostics > Support Workbench** under the **Automatic Storage Management** target menu at the top of the page.

[Figure 13](#) shows the Oracle ASM Support Workbench page with the **Problems** tab displayed. You can view information about current and past problems in this tab. On this page, you have options to view additional details and create a package that you can send to Oracle Support Services.

Figure 13 Oracle Automatic Storage Management Support Workbench Problems

Automatic Storage Management

Host: adc2171647.us.oracle.com > Automatic Storage Management: myASM > Support Workbench

Support Workbench

Page Refreshed **January 23, 2013 3:27:48 PM PST** [Refresh](#)

Problems (2) | [Checker Findings \(0\)](#) | [Packages \(0\)](#)

New Problems in Last 24 Hours: 0 All Active Problems: 0 All Problems: 2
 New Incidents in Last 24 Hours: 0 All Active Incidents: 0 All Incidents: 4

View: [Last 2 Days](#) Filter by problem key: [Go](#) [Advanced Search](#)

[View](#) [Package](#)

[Select All](#) | [Select None](#) | [Show All Details](#) | [Hide All Details](#)

Select	Details	ID	Description	Number Of Incidents	Last Incident	Last Comment	Active	Packaged	SR#
<input type="checkbox"/>	Show	1	ORA 7445 [sentimedop]	3	January 22, 2013 12:26:28 PM PST		No	No	
<input type="checkbox"/>	Show	2	ORA 7445 [read]	1	January 22, 2013 12:23:57 PM PST		No	No	

[Critical Error Timeline](#)

Related Links

[Alert Log Contents](#) [Create User-Reported Problem](#) [Incident Packaging Configuration](#)
[Checker Central](#) [Support Workbench \(orcl.us.oracle.com\)](#)

Support Workbench guides you through the packaging process as follows:

1. To create a package, select an incident and click **Package** on the Support Workbench Problems page. The Support Workbench **Select packaging mode** page of the wizard displays.
2. On the **Select packaging mode** page, select either the **Quick** or **Custom** packaging mode.
3. Depending on the packaging mode chosen, you are presented with various entry fields and options as you click **Next** through the wizard.

The wizard guides you through the packaging process using a series of steps that include:

- Viewing and editing the contents of the package
- Viewing and editing the manifest of the package
- Adding additional diagnostic details
- Scheduling the generation and uploading of the package

You can view and edit information about packages created for problems on the Support Workbench **Packages** tab, as shown in [Figure 14](#). You can check findings on the Support Workbench **Checker Findings** tab.

Figure 14 Oracle Automatic Storage Management Support Workbench Packages

Host: adc2171647.us.oracle.com > Automatic Storage Management: myASM > Support Workbench

Support Workbench

Page Refreshed **January 24, 2013 8:25:09 AM PST** [Refresh](#)

Problems (2) | Checker Findings (0) | **Packages (2)**

Active 1 Contents Finalized 0
 Upload File Generated 1 Sent to Oracle 0

Search [Go](#)

[Delete](#)

Select All | Select None

Select	Name	Status	Description	Main Problem Keys	Created
<input type="checkbox"/>	ORA7445se_20130124081215	Active		ORA 7445 [sentimedop]	January 24, 2013 8:12:37 AM PST
<input type="checkbox"/>	ORA7445re_20130124075647	Upload File Generated	my_new_pkg	ORA 7445 [read]	January 24, 2013 7:58:03 AM PST

Related Links

[Alert Log Contents](#) [Create User-Reported Problem](#) [Incident Packaging Configuration](#)
[Checker Central](#) [Support Workbench \(orcl.us.oracle.com\)](#)

See Also:

Oracle Database Administrator's Guide for information about viewing problems with Oracle Enterprise Manager Support Workbench

Monitoring Oracle Flex ASM

Oracle Enterprise Manager provides functionality to monitor your Oracle Flex ASM configuration. For more information about Oracle Flex ASM, refer to “[Managing Oracle Flex ASM](#)”.

[Figure 15](#) shows the top portion of the Oracle Flex ASM home page. On the page, you can view and administer components of the Oracle Flex ASM configuration.

Figure 15 Oracle Flex ASM Home Page

+ASM_slc00duzdvc-r Logged in as SYS slc00dvb.us.oracle.com

Cluster ASM

Host: slc00dvb.us.oracle.com > Cluster ASM: +ASM_slc00duzdvc-r Logged in as SYS / SYSASM

Cluster ASM

Home | Performance | Disk Groups | Configuration | Users | ASM Cluster File System

Data Retrieved Nov 29, 2012 9:08:59 AM PST [Refresh](#)

General

[Startup/Shutdown](#)

Current Status Up
 Instances 3 (3)
 Up Since Nov 29, 2012 2:05:57 AM PST
 Availability (%) 100
 (Last 24 hours)
 Cluster slc00duzdvc-r
 Version 12.1.0.1.0
 Master Agent Host slc00dvb.us.oracle.com
 Oracle Home /scratch/oh121126
 Flex Enabled Yes

Disk Group Usage (GB)

Disk Group	Unallocated (GB)	System (GB)	ASM (GB)
OCRDG	~2.8	~0.2	~0.0
BACKUP	~3.8	~0.2	~0.0
DATACORE	~5.8	~0.2	~0.0

Connected Databases

[Figure 16](#) shows the Oracle Flex ASM Members page. On the page, you can view all the members of the Oracle Flex ASM configuration.

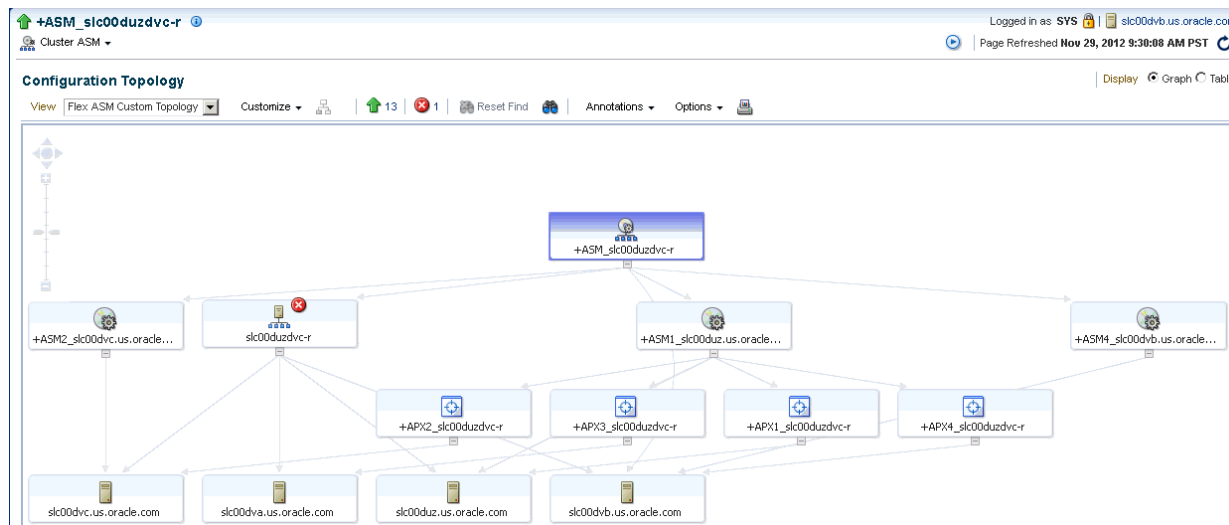
Figure 16 Oracle Flex ASM Members Page

Name	Type
+APX1_slc00duzdvc-r	ASM Proxy
+APX2_slc00duzdvc-r	ASM Proxy
+APX3_slc00duzdvc-r	ASM Proxy
+APX4_slc00duzdvc-r	ASM Proxy
+ASM1_slc00duz.us.oracle.com	Automatic Storage Management
+ASM2_slc00dvc.us.oracle.com	Automatic Storage Management
+ASM4_slc00dvh.us.oracle.com	Automatic Storage Management

Availability Definition
 Definition **The redundancy systems status is up if 1 member targets are up**

Figure 17 shows the Oracle Flex ASM Topology page. On the page, you can view the topology of the Oracle Flex ASM configuration.

Figure 17 Oracle Flex ASM Topology Page



For information about Oracle Flex ASM, refer to “[Managing Oracle Flex ASM](#)”.

Performing Oracle ASM Data Migration with RMAN

This chapter describes how to migrate data into and out of Oracle Automatic Storage Management (Oracle ASM) storage with Recovery Manager (RMAN).

This chapter includes the following topics:

- [Overview of Oracle ASM Data Migration](#)
- [Preparing to Migrate the Database to Oracle ASM Using RMAN](#)
- [Migrating the Database to Oracle ASM Using RMAN](#)
- [Migrating a Database from Oracle ASM to Alternative Storage](#)
- [Moving Data Files Between Oracle ASM Disk Groups Using RMAN](#)

The procedures in this chapter cover an Oracle ASM standalone environment on a Linux platform. File locations and procedures may be different for different Oracle configurations and on other operating system platforms.

See Also:

- *Oracle Database Backup and Recovery User's Guide* for complete information about using RMAN
 - Operating system-specific documentation for migrating data in and out of Oracle ASM on specific platforms
 - *Oracle Clusterware Administration and Deployment Guide* for information about managing and migrating Oracle Cluster Registry and voting files
 - *Oracle Real Applications Cluster Administration and Deployment Guide* for migrating data in and out of Oracle ASM in an Oracle RAC configuration
-

Overview of Oracle ASM Data Migration

This section explains the basic concepts and tasks involved in migrating data to and from Oracle ASM.

This section includes the following topics:

- [Purpose of Oracle ASM Data Migration](#)
- [Basic Concepts of Oracle ASM Data Migration](#)

- [Basic Steps of Data Migration to Oracle ASM Using RMAN](#)

Purpose of Oracle ASM Data Migration

Alternatives to Oracle ASM storage include file systems, raw disks, and SAN configurations. Oracle ASM includes numerous benefits over these storage alternatives, including performance optimization, redundancy protection, and load balancing. You do not need a third-party Logical Volume Manager because Oracle ASM manages disks for you. Oracle Real Application Clusters (Oracle RAC) databases benefit from Oracle ASM because it provides ready-made shared storage.

If a database currently uses a storage system other than Oracle ASM, then you can migrate all or part of the database into Oracle ASM, thereby simplifying database administration. You can also migrate a fast recovery area to Oracle ASM.

Native operating system commands such as Linux `cp` or Windows `COPY` cannot write or read files in Oracle ASM storage. Because RMAN can read and write Oracle ASM files, you can use RMAN to copy data files into and out of Oracle ASM storage or between Oracle ASM disk groups. This technique is useful if you must store backups on user-managed disks.

Basic Concepts of Oracle ASM Data Migration

You can migrate data to Oracle ASM with RMAN even if you are not using RMAN as your primary backup tool. The migration requires one RMAN database backup.

If you have sufficient disk space to hold the entire database both in Oracle ASM and alternative storage systems, then you can move a database directly into Oracle ASM. If you do not have sufficient storage, then you can back the database up to tape, create an Oracle ASM disk group that uses old disk space, and restore the database from tape to Oracle ASM.

After you set the location of the new recovery area, existing backups remain in the old recovery area and count against the total disk quota of the recovery area. The backups are deleted from the old recovery area when space is needed. These backups are usable by RMAN. It is not necessary to move legacy backups to the new Oracle ASM recovery area unless you need disk space. To free space consumed by files in the old recovery area, you can back them up to tape or migrate them to the Oracle ASM recovery area.

Note:

A foreign archived redo log is a log received by a logical standby database for a LogMiner session. Foreign archived redo logs cannot be migrated. Unlike normal archived logs, foreign archived logs have a different internal database identifier (DBID). For this reason, they cannot be backed up or restored on a logical standby database.

Migrating a database from Oracle ASM to an alternative storage system is similar to migration from an alternative storage system to Oracle ASM. The primary change is to modify each step to refer to file locations in the alternative storage system.

Basic Steps of Data Migration to Oracle ASM Using RMAN

This section discusses the process of migrating the entire database and fast recovery area from alternative storage to Oracle ASM using RMAN.

The fast recovery area is an optional disk location that you can use to store recovery-related files such as control file and online redo log copies, archived redo log files, flashback logs, and RMAN backups. Oracle Database and RMAN manage the files in the fast recovery area automatically. You can specify the disk quota, which is the user-specified maximum size of the fast recovery area. When the disk quota is reached, Oracle automatically deletes files that are no longer needed.

Flashback logs are Oracle-generated logs used to perform flashback database operations. The database can only write flashback logs to the fast recovery area. Flashback logs are written sequentially and are not archived. They cannot be backed up to disk.

To migrate the entire database and fast recovery area from alternative storage to Oracle ASM, perform the following steps:

1. Back up the database and server parameter file, and disable Oracle Flashback Database.

The Oracle Flashback Database option returns the entire database to a prior consistent System Change Number (SCN) with the `FLASHBACK DATABASE` command in RMAN or SQL. A database flashback is different from traditional media recovery because it does not involve the restore of physical files, instead restoring your current data files to past states using saved images of changed data blocks. This feature uses flashback logs and archived redo logs.

This step is described in [“Preparing to Migrate the Database to Oracle ASM Using RMAN”](#).

2. Restore files to Oracle ASM, recover the database, and optionally migrate the fast recovery area to Oracle ASM.

This step is described in [“Migrating the Database to Oracle ASM Using RMAN”](#).

To migrate files from Oracle ASM to alternative storage, see [“Migrating a Database from Oracle ASM to Alternative Storage”](#).

Preparing to Migrate the Database to Oracle ASM Using RMAN

This section explains how to prepare the database for migration. This section makes the following assumptions:

- You want to migrate the database to two Oracle ASM disk groups: `+DATA` for the database and `+FRA` for the fast recovery area.
- The database to be migrated to Oracle ASM storage is named `mydb`.

To prepare the database for Oracle ASM migration:

1. If the `COMPATIBLE` initialization parameter setting for the database is less than `11.0.0`, then make any read-only transportable tablespaces read/write.

Read-only transportable tablespaces cannot be migrated because RMAN cannot back them up.

2. If the database is a physical standby database, and if managed recovery is started, then stop managed recovery.

A physical standby database is a copy of a production database that you can use for disaster protection.

For example, connect SQL*Plus to the database with SYSBACKUP privileges (rather than SYSDBA privileges) to enforce the separation of duty security model, and run the following statement to stop managed recovery:

```
SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL;
```

Keep this terminal window open.

3. Copy the server parameter file or initialization parameter file to a temporary location.

The following example uses an operating system utility to copy the server parameter file:

```
$ cp spfileMYDB.ora orig_spfileMYDB.ora
```

4. In a new terminal window, start RMAN session and connect as TARGET to the database to be migrated. Optionally, connect to a recovery catalog. Connect with SYSBACKUP privileges to enforce the separation of duty security model.

5. Back up the data files to the Oracle ASM disk group.

The following example uses a RUN command to make a level 0 incremental backup and allocates four channels to increase the backup speed. A level 0 incremental backup is an RMAN incremental backup that backs up all data blocks in the data files being backed up. An incremental backup at level 0 is identical in content to a full backup, but unlike a full backup the level 0 backup is considered a part of the incremental backup strategy.

An incremental backup is a RMAN backup in which only modified blocks are backed up. Incremental backups are classified by **level**. A level 0 incremental backup performs the same function as a full backup in that they both back up all blocks that have ever been used. The difference is that a full backup does not affect blocks backed up by subsequent incremental backups, whereas an incremental backup affects blocks backed up by subsequent incremental backups.

A full backup is a non-incremental RMAN backup. Full does not refer to how much of the database is backed up, but to the fact that the backup is not incremental. Consequently, you can make a full backup of one data file.

Increase or decrease this number accordingly. The format clause specifies +DATA, which is the name of the Oracle ASM disk group to be used for storing the database.

```
RUN
{
  ALLOCATE CHANNEL dev1 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev2 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev3 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev4 DEVICE TYPE DISK;
  BACKUP AS COPY
    INCREMENTAL LEVEL 0
    DATABASE
    FORMAT '+DATA'
    TAG 'ORA_ASM_MIGRATION';
}
```

6. If block change tracking is enabled for the database, then optionally make a level 1 incremental backup that you can use later to recover the database copy.

Block change tracking is a database option that causes Oracle to track data file blocks affected by each database update. The tracking information is stored in a block change tracking file. When block change tracking is enabled, RMAN uses

the record of changed blocks from the change tracking file to improve incremental backup performance by only reading those blocks known to have changed, instead of reading data files in their entirety.

The following example makes an incremental level 1 copy of the level 0 backup created in the previous step:

```
RUN
{
  ALLOCATE CHANNEL dev1 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev2 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev3 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev4 DEVICE TYPE DISK;
  BACKUP INCREMENTAL LEVEL 1
    FOR RECOVER OF COPY WITH TAG 'ORA_ASM_MIGRATION'
    DATABASE;
}
```

7. If the database is in ARCHIVELOG mode, and if the database is open, then archive the online logs.

The following example uses the SQL command to archive the current redo logs:

```
RMAN> SQL "ALTER SYSTEM ARCHIVE LOG CURRENT";
```

8. If the database instance is currently using a server parameter file, then back it up.

The following example backs up the server parameter file:

```
RMAN> BACKUP AS BACKUPSET SPFILE;
```

9. If block change tracking is enabled, then disable it.

The following command disables block change tracking:

```
RMAN> SQL "ALTER DATABASE DISABLE BLOCK CHANGE TRACKING";
```

10. If Flashback Database is enabled, then disable it and drop any guaranteed restore points.

Note:

If you are not migrating the fast recovery area, then skip this step.

Disabling Oracle Flashback Database is necessary because you cannot migrate flashback logs to Oracle ASM. The following command disables Flashback Database:

```
RMAN> SQL "ALTER DATABASE FLASHBACK OFF";
```

The following command drops the guaranteed restore point named Q106:

```
RMAN> SQL "DROP RESTORE POINT Q106";
```

11. Shut down the database consistently.

The following command shuts down the database:

```
RMAN> SHUTDOWN IMMEDIATE;
```

Migrating the Database to Oracle ASM Using RMAN

The following procedure is intended to minimize database downtime. The steps differ slightly depending on whether you are migrating a primary or standby database. The

procedure makes the same assumptions described in “[Preparing to Migrate the Database to Oracle ASM Using RMAN](#)”. If you are not migrating the recovery area to Oracle ASM, then you must modify some steps, which are noted.

Note:

The following procedure switches between SQL*Plus and RMAN, so keep a terminal window open for each utility.

To migrate the database to Oracle ASM:

1. Follow the steps in “[Preparing to Migrate the Database to Oracle ASM Using RMAN](#)”.
2. Restore or create a server parameter file in Oracle ASM storage.

The steps depend on whether the database is using a server parameter file:

- If the database is using a server parameter file, then restore it to the Oracle ASM disk group with the following commands, where *sid* is the SID of the instance:

```
RMAN> STARTUP MOUNT;
RMAN> RESTORE SPFILE TO '+DATA/spfilesid.ora';
RMAN> SHUTDOWN IMMEDIATE;
```

- If the database is not using a server parameter file, then create one in Oracle ASM. Run the CREATE SPFILE command in SQL*Plus as follows, where *sid* is the SID of the database:

```
SQL> CREATE SPFILE='+DATA/spfilesid.ora' FROM PFILE='?/dbs/initsid.ora';
```

3. Set Oracle Managed Files initialization parameters to Oracle ASM locations.

Note:

If you are not migrating the fast recovery area, then do not change the DB_RECOVERY_FILE_DEST and DB_RECOVERY_FILE_DEST_SIZE initialization parameter settings. However, you must set DB_CREATE_ONLINE_LOG_DEST_n parameter to an Oracle ASM location for migration of the online redo logs.

Set the DB_CREATE_FILE_DEST and optional DB_CREATE_ONLINE_LOG_DEST_n initialization parameters to Oracle ASM disk groups. If the database uses a recovery area, then change the recovery area location to the Oracle ASM disk group. Also, change the recovery area size.

Run commands in SQL*Plus as shown in the following example. The example assumes that the size of the fast recovery area is 100 GB and specifies the disk group +FRA for the fast recovery area.

```
SQL> STARTUP FORCE NOMOUNT;
SQL> ALTER SYSTEM SET DB_CREATE_FILE_DEST='+DATA' SID='*';
SQL> ALTER SYSTEM SET DB_RECOVERY_FILE_DEST_SIZE=100G SID='*';
SQL> ALTER SYSTEM SET DB_RECOVERY_FILE_DEST='+FRA' SID='*';
```

4. Set the CONTROL_FILES initialization parameter to Oracle ASM locations.

If you are migrating the fast recovery area, then enter the following commands in SQL*Plus to restart the database instance and set the control file locations to disk groups +DATA and +FRA:

```
SQL> STARTUP FORCE NOMOUNT;
SQL> ALTER SYSTEM SET CONTROL_FILES='+DATA','+FRA' SCOPE=SPFILE SID='*';
```

If you are not migrating the fast recovery area, then enter the following commands in SQL*Plus to restart the database instance and set the control file locations to disk group +DATA:

```
SQL> STARTUP FORCE NOMOUNT;
SQL> ALTER SYSTEM SET CONTROL_FILES='+DATA','+DATA' SCOPE=SPFILE SID='*';
```

5. Migrate the control file to Oracle ASM and mount the control file.

Switch to the RMAN terminal to restore the control file. In the following example, *original_cf_name* is a control file name in the initialization parameter file before migration:

```
RMAN> STARTUP FORCE NOMOUNT;
RMAN> RESTORE CONTROLFILE FROM 'original_cf_name';
RMAN> ALTER DATABASE MOUNT;
```

6. Migrate the data files to Oracle ASM.

Use RMAN to switch to the database copy that you created in step 5 "Back up the data files to the Oracle ASM disk group" in "[Preparing to Migrate the Database to Oracle ASM Using RMAN](#)". The switch renames all the data files to files on Oracle ASM disk groups. Afterward, recover the database. If incremental backups were taken, then RMAN applies them during recovery. For example, enter the following commands at the RMAN prompt:

```
SWITCH DATABASE TO COPY;
RUN
{
  ALLOCATE CHANNEL dev1 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev2 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev3 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev4 DEVICE TYPE DISK;
  RECOVER DATABASE;
}
```

7. If the database uses block change tracking or Flashback Database, then enable these features.

Note:

If you are not migrating the recovery area, then you do not enable Flashback Database unless you had disabled it previously.

For example, enter the following statements in SQL*Plus:

```
SQL> ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE '+DATA';
SQL> ALTER DATABASE FLASHBACK ON;
```

8. Place the database in its normal operation mode.

The normal operational mode depends on whether the database is a primary or standby database:

- If the database is a primary database, then open it as follows:

```
SQL> ALTER DATABASE OPEN;
```

- If the database is a standby database, then resume managed recovery mode as follows:

```
SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE;
```

9. Drop the tempfiles and re-create them in Oracle ASM.

Use SQL*Plus to re-create the tempfiles. In the following example, the name of the tempfile in the original storage is *tempfile_name*. The name of the temporary tablespace is *temp_tbs_name*.

```
SQL> ALTER DATABASE TEMPFILE 'tempfile_name' DROP;
SQL> ALTER TABLESPACE temp_tbs_name ADD TEMPFILE;
```

10. Migrate the online redo log files.

If this is a primary database, then add new log group members in Oracle ASM and drop the old members. You can use the following PL/SQL script to migrate the online redo log groups into an Oracle ASM disk group. The PL/SQL script assumes that the Oracle Managed Files initialization parameters specified in step 3 "Set Oracle Managed Files initialization parameters to Oracle ASM locations" in "Migrating the Database to Oracle ASM Using RMAN" are set.

11. Optionally, migrate backups and copies in the old fast recovery area to Oracle ASM as follows:

- If foreign archived logs exists in the recovery area, then you cannot migrate them to Oracle ASM. Run the following command at the RMAN prompt:

```
RMAN> DELETE ARCHIVELOG ALL;
```

- Back up archived redo log files, backup sets, and data file copies to Oracle ASM. For example, run the following command at the RMAN prompt:

```
RUN
{
  ALLOCATE CHANNEL dev1 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev2 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev3 DEVICE TYPE DISK;
  ALLOCATE CHANNEL dev4 DEVICE TYPE DISK;

  BACKUP AS COPY ARCHIVELOG ALL DELETE INPUT;
  BACKUP BACKUPSET ALL DELETE INPUT;
  BACKUP AS COPY DATAFILECOPY ALL DELETE INPUT;
}
```

Example 1 Migrating the online redo logs

```
SET SERVEROUTPUT ON;
DECLARE
  CURSOR rlc IS
    SELECT GROUP# GRP, THREAD# THR, BYTES, 'NO' SRL
    FROM V$LOG
    UNION
    SELECT GROUP# GRP, THREAD# THR, BYTES, 'YES' SRL
    FROM V$STANDBY_LOG
    ORDER BY 1;
  stmt VARCHAR2(2048);
BEGIN
  FOR rlcRec IN rlc LOOP
    IF (rlcRec.srl = 'YES') THEN
      stmt := 'ALTER DATABASE ADD STANDBY LOGFILE THREAD ' ||
        rlcRec.thr || ' SIZE ' || rlcRec.bytes;
      EXECUTE IMMEDIATE stmt;
```

```

        stmt := 'ALTER DATABASE DROP STANDBY LOGFILE GROUP ' || rlcRec.grp;
        EXECUTE IMMEDIATE stmt;
    ELSE
        stmt := 'ALTER DATABASE ADD LOGFILE THREAD ' ||
            rlcRec.thr || ' SIZE ' || rlcRec.bytes;
        EXECUTE IMMEDIATE stmt;
    BEGIN
        stmt := 'ALTER DATABASE DROP LOGFILE GROUP ' || rlcRec.grp;
        DBMS_OUTPUT.PUT_LINE(stmt);
        EXECUTE IMMEDIATE stmt;
    EXCEPTION
        WHEN OTHERS THEN
            EXECUTE IMMEDIATE 'ALTER SYSTEM SWITCH LOGFILE';
            EXECUTE IMMEDIATE 'ALTER SYSTEM CHECKPOINT GLOBAL';
            EXECUTE IMMEDIATE stmt;
    END;
END IF;
END LOOP;
END;
/

```

Migrating a Database from Oracle ASM to Alternative Storage

Migrating a database from Oracle ASM to an alternative storage system is essentially the reverse of the migration to Oracle ASM. Modify the steps in [“Preparing to Migrate the Database to Oracle ASM Using RMAN”](#) and [“Migrating the Database to Oracle ASM Using RMAN”](#) as follows:

- If the procedure specifies Oracle Managed Files locations, then alter the procedure to use locations in alternative storage.
- If the `FORMAT` clause of the `BACKUP` command specifies an Oracle ASM location, then change the backup format to an alternative storage location.
- If a file name used in a SQL statement is an Oracle ASM location, then change it to a file name in the alternative storage location.

Moving Data Files Between Oracle ASM Disk Groups Using RMAN

You may want to move an active data file in an `ARCHIVELOG` mode database from one Oracle ASM disk group to another. You can use `RMAN BACKUP AS COPY` to copy the data file to the new disk group and `SET NEWNAME` and `SWITCH` commands to rename the data file in the control file.

You can also use the `ALTER DATABASE MOVE DATAFILE` SQL statement to move data files. For information about moving data files online with `ALTER DATABASE MOVE DATAFILE`, refer to [“Moving Data Files Between Disk Groups With ALTER DATABASE”](#).

For this scenario using RMAN, assume that you are using disk groups `DATA` and `USERDATA` and you want to move the data file `users.261.689589837` to disk group `USERDATA`. Ensure that `ARCHIVELOG` mode is enabled for the database before beginning the procedure to move data files.

To move a data file from one Oracle ASM disk group to another disk group using the `RMAN BACKUP AS COPY` procedure with the `SET NEWNAME` and `SWITCH` commands, perform the following steps.

1. Start RMAN and connect to the target database.

For example:

```
$ rman
RMAN> CONNECT TARGET SYS@orcl
target database Password: XXXXXXXXXX
connected to target database: ORCL (DBID=1217369048)
```

2. Generate a report that shows the names of the data files.

Run the following REPORT command after connecting RMAN to the target database. Note the data file name of the file to be moved.

For example:

```
RMAN> REPORT SCHEMA;

Report of database schema for database with db_unique_name ORCL

List of Permanent Datafiles
=====
File Size(MB) Tablespace          RB segs Datafile Name
-----
1      740      SYSTEM                ***      +DATA/orcl/datafile/system.
258.689589737
2      570      SYSAUX                  ***      +DATA/orcl/datafile/sysaux.
259.689589785
3      55       UNDOTBS1                ***      +DATA/orcl/datafile/
undotbs1.260.689589831
4      5        USERS                   ***      +DATA/orcl/datafile/users.
261.689589837

List of Temporary Files
=====
File Size(MB) Tablespace          Maxsize(MB) Tempfile Name
-----
1      20       TEMP                    32767    +DATA/orcl/tempfile/temp.
262.689589851
```

3. Back up the data file to the new Oracle ASM disk group.

Run the BACKUP AS COPY command to back up the data file on DATA to USERDATA.

For example:

```
RMAN> BACKUP AS COPY
      DATAFILE "+DATA/orcl/datafile/users.261.689589837"
      FORMAT    "+USERDATA" ;

Starting backup at 16-JUN-09
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=51 device type=DISK
channel ORA_DISK_1: starting datafile copy
input datafile file number=00004 name=+DATA/orcl/datafile/users.
261.689589837
output file name=+USERDATA/orcl/datafile/users.256.689682663
tag=TAG20090616T103101 RECID=13 STAMP=689682663
channel ORA_DISK_1: datafile copy complete, elapsed time: 00:00:01
Finished backup at 16-JUN-09
```

You could also specify the data file by the data file number and data file type.

For example:

```
BACKUP AS COPY
      DATAFILE 4
      FORMAT    "+USERDATA" ;
```

4. Offline the data file that you intend to move to a new disk group.

Run the following SQL command in the RMAN client. Use two single quotation marks around the name of the data file, not double quotation marks.

For example:

```

RMAN> SQL "ALTER DATABASE DATAFILE
        '+DATA/orcl/datafile/users.261.689589837' OFFLINE";

sql statement: ALTER DATABASE DATAFILE
        '+DATA/orcl/datafile/users.261.689589837' OFFLINE

```

5. Point the control file to the newly created copy of the data file.

Run the SWITCH . . . TO COPY command in the RMAN client. The TO COPY option of SWITCH switches the data file to the most recent copy of the data file.

For example:

```

RMAN> SWITCH DATAFILE "+DATA/orcl/datafile/users.261.689589837" TO COPY;

datafile 4 switched to datafile copy
        "+USERDATA/orcl/datafile/users.256.689682663"

```

The output of this command displays the new name of the data file.

6. Recover the renamed data file.

Run the RECOVER command in the RMAN client.

For example:

```

RMAN> RECOVER DATAFILE "+USERDATA/orcl/datafile/users.256.689682663";

Starting recover at 16-JUN-09
using channel ORA_DISK_1
starting media recovery
media recovery complete, elapsed time: 00:00:01
Finished recover at 16-JUN-09

```

7. Bring the data file online.

Run the SQL command in the RMAN client. Use two single quotation marks around the name of the data file, not double quotation marks.

For example:

```

RMAN> SQL "ALTER DATABASE DATAFILE
        '+USERDATA/orcl/datafile/users.256.689682663' ONLINE";

sql statement: ALTER DATABASE DATAFILE
        '+USERDATA/orcl/datafile/users.256.689682663' ONLINE

```

8. Delete the data file copy from the original Oracle ASM disk group.

In this scenario, +DATA/orcl/datafile/users.261.689589837 is the original data file in DATA. Because you issued SET NEWNAME and SWITCH commands for this data file, the original file is now recorded in the RMAN repository as a data file copy. Run a DELETE command in the RMAN client to remove this file.

For example:

```

RMAN> DELETE DATAFILECOPY "+DATA/orcl/datafile/users.261.689589837";

released channel: ORA_DISK_1
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=51 device type=DISK
List of Datafile Copies
=====

```

Key	File S	Completion Time	Ckp SCN	Ckp Time
14	4	A 16-JUN-09	864471	16-JUN-09

Name: +DATA/orcl/datafile/users.261.689589837
Tag: TAG20090615T084217

Do you really want to delete the above objects (enter YES or NO)? y
deleted datafile copy
datafile copy file name=+DATA/orcl/datafile/users.261.689589837 RECID=14
STAMP=689683255
Deleted 1 objects

Managing Oracle ASM With ASMCA

Oracle ASM Configuration Assistant (ASMCA) supports installing and configuring Oracle ASM instances, Oracle ASM disk groups, Oracle ASM Dynamic Volume Manager (Oracle ADVM) volumes, and Oracle Automatic Storage Management Cluster File System (Oracle ACFS) file systems. In addition, you can use the ASMCA command-line interface.

This chapter discusses the following topics:

- [Getting Started With the ASMCA GUI Tool](#)
- [Managing Instances and Disk Groups With ASMCA](#)
- [ASMCA Command-Line Interface](#)

For information about managing Oracle ACFS and Oracle ADVM with ASMCA, refer to [Managing Oracle ACFS and Oracle ADVM With ASMCA](#). For information about using ASMCA to convert to Oracle Flex ASM, refer to “[About Converting to Oracle Flex ASM](#)”.

Getting Started With the ASMCA GUI Tool

To start ASMCA, enter `asmca` at a command prompt inside the Oracle Grid Infrastructure home. For example:

```
$ asmca
```

The GUI tool displays and attempts to connect to the Oracle ASM instance identified with the Oracle system identifier (SID) set to `+ASM`.

- If ASMCA detects an Oracle ASM instance that is not running, then ASMCA prompts whether you want to start the instance.
- If ASMCA detects an Oracle ASM instance from a previous release, then ASMCA prompts whether you want to upgrade the instance. Oracle recommends that you respond `No` to this prompt.

An Oracle ASM instance should be upgraded with Oracle Universal Installer (OUI). OUI automatically defaults to upgrade mode when it detects an Oracle ASM instance at a previous release level.

To continue the upgrade process with ASMCA, see “[Upgrading an Oracle ASM Instance with ASMCA](#)”. If you need help with upgrading an Oracle ASM instance, contact Oracle Support Services.

The **Instances** tab functionality and some menu options of ASMCA are only available in an Oracle RAC configuration.

To start the command-line ASMCA, see “[ASMCA Command-Line Interface](#)”.

Managing Instances and Disk Groups With ASMCA

This section contains the following topics:

- [Creating Oracle ASM Instances with ASMCA](#)
- [Upgrading an Oracle ASM Instance with ASMCA](#)
- [Managing Disk Groups with ASMCA](#)

Creating Oracle ASM Instances with ASMCA

Oracle ASM Configuration Assistant enables you to create an Oracle ASM instance if an Oracle ASM instance is not found on the host, as shown in [Figure 1](#).

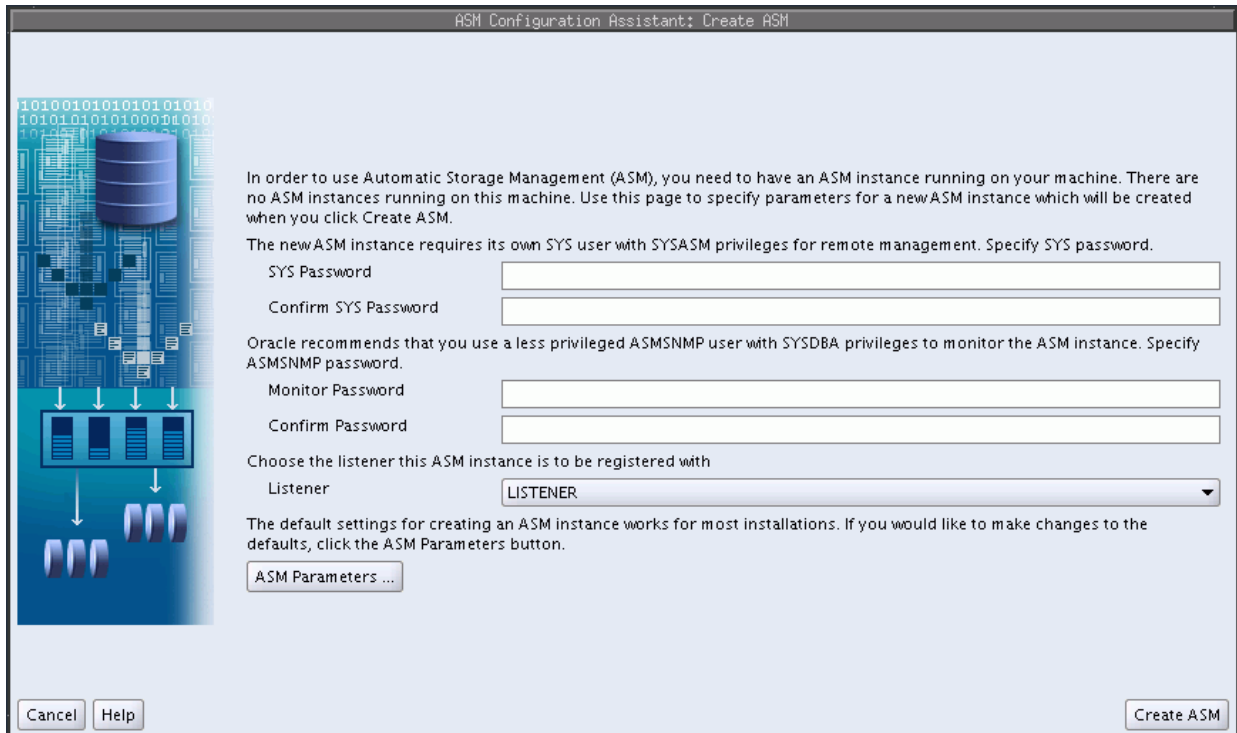
On the **Create ASM** page, you enter the `SYS` password for the administrator of the Oracle ASM instance and the password for the `ASMSNMP` user that can monitor this Oracle ASM instance. `ASMSNMP` is a less privileged user that is primarily used to monitor Oracle ASM instances.

See Also:

- *Oracle Grid Infrastructure Installation Guide* for information about installing Oracle ASM
 - *Oracle Database Installation Guide* for information about reviewing database accounts and passwords
-
-

You can select the listener with which to register this Oracle ASM instance. Click **ASM Parameters** to update the initialization parameters for the Oracle ASM instance.

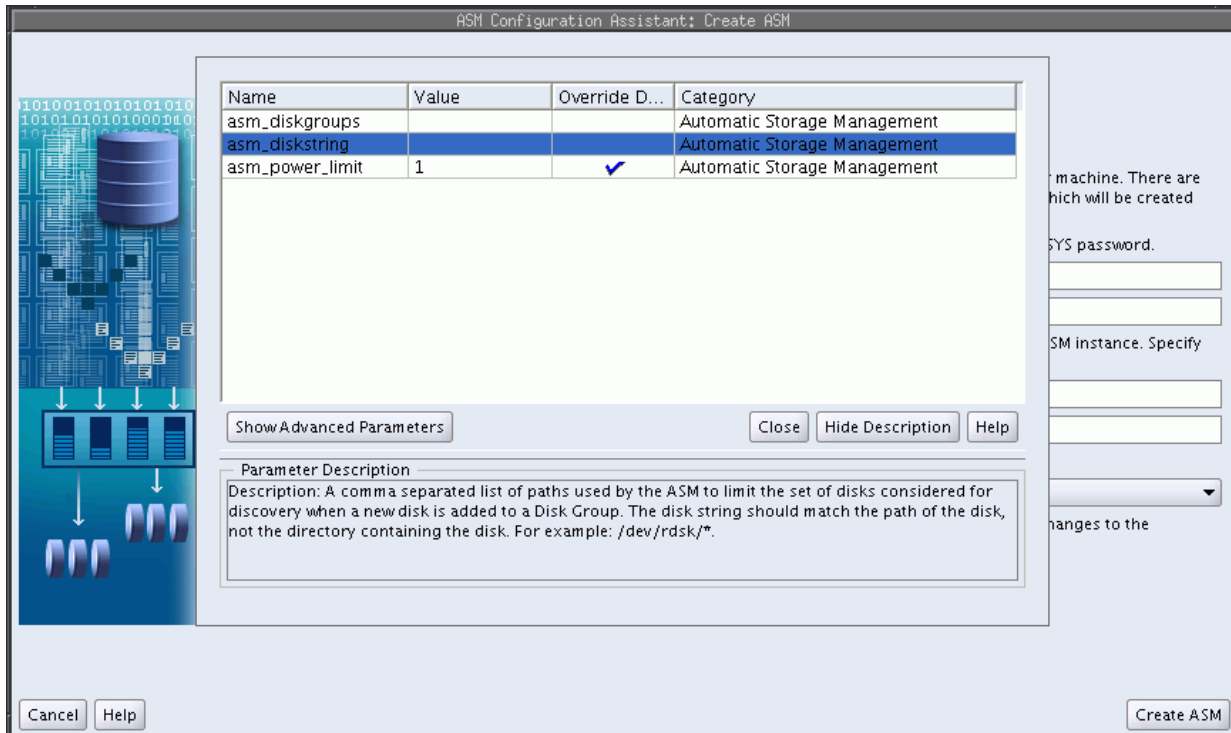
Figure 1 Oracle ASM Configuration Assistant Create ASM Page



When you can click **ASM Parameters** in the **Create ASM** page, you can update initialization parameters for an Oracle ASM instance on the Oracle ASM Configuration Assistant page, as shown in [Figure 2](#).

For information about Oracle ASM instance initialization parameters, see [“Initialization Parameters for Oracle ASM Instances”](#).

Figure 2 Oracle ASM Configuration Assistant Create ASM Page



Upgrading an Oracle ASM Instance with ASMCA

Oracle ASM Configuration Assistant also enables you to upgrade an existing Oracle ASM instance to the current software level. However, the recommended practice is to upgrade an Oracle ASM instance with Oracle Universal Installer (OUI). OUI automatically defaults to upgrade mode when it detects an Oracle ASM instance at a previous release level.

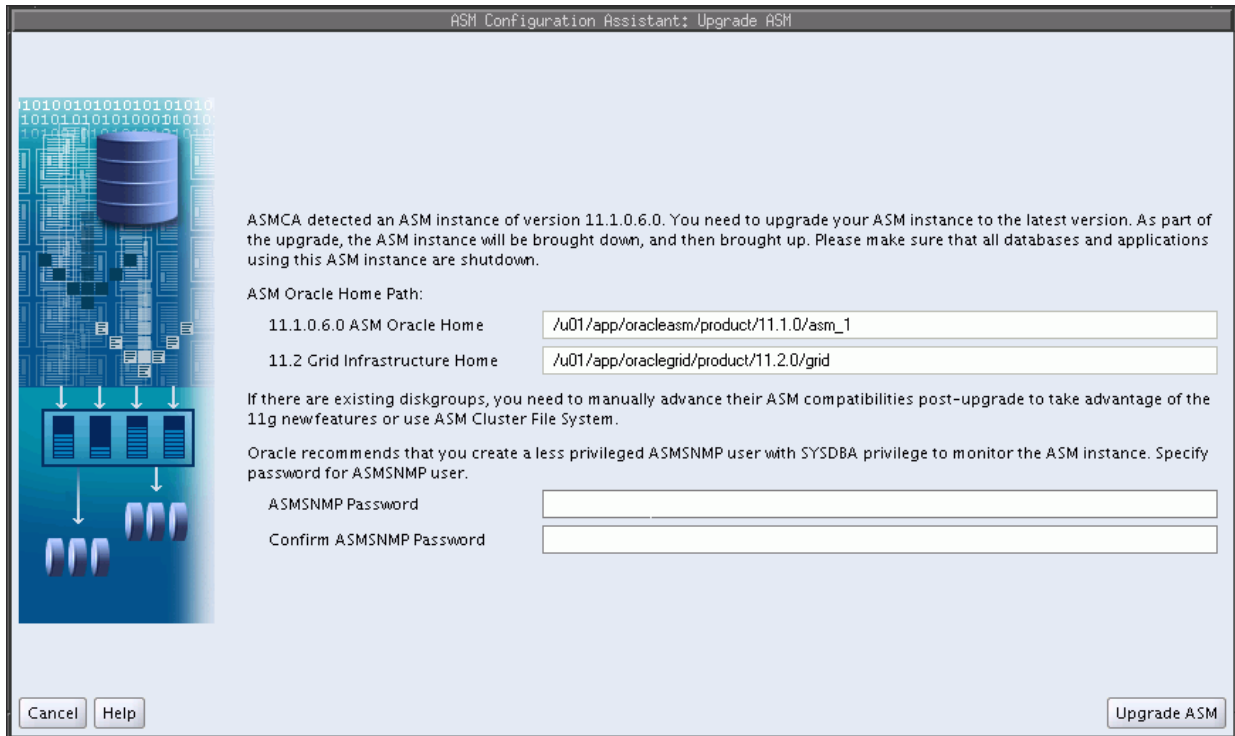
If Oracle Clusterware has been upgraded, then there is no need to upgrade the Oracle ASM instance in that Oracle Grid Infrastructure home. Oracle ASM is usually upgraded as part of the Oracle Clusterware upgrade.

See Also:

- *Oracle Grid Infrastructure Installation Guide* for information about installing and upgrading Oracle Grid Infrastructure
 - Articles at [My Oracle Support \(https://support.oracle.com\)](https://support.oracle.com) for information about upgrading Oracle ASM
-
-

Note:

The procedure described in this section upgrades the Oracle ASM instance only. Oracle Database, and Oracle Enterprise Manager, will not have the latest features. To upgrade Oracle Database, see *Oracle Database Upgrade Guide*.

Figure 3 Oracle ASM Configuration Assistant Upgrade ASM Page

After upgrading an Oracle ASM instance, you can copy or move an Oracle ASM SPFILE. After copying or moving the SPFILE, you must restart the instance with the SPFILE in the new location to use that SPFILE. For information, see “[About Backing Up_ Copying_ and Moving an Oracle ASM Initialization Parameter File](#)”.

See Also:

- *Oracle Database Upgrade Guide* for information about upgrading Oracle Database
 - *Oracle Grid Infrastructure Installation Guide* for information about installing Oracle Grid Infrastructure and performing a rolling upgrade of Oracle ASM
-

Managing Disk Groups with ASMCA

Oracle ASM Configuration Assistant enables you to configure or create Oracle ASM disk groups with the **Configure ASM Disk Groups** tab, as shown in [Figure 4](#). The disk group tab displays selected details about the disk group, such as name, size, free space, usable space, redundancy level, and state of the disk group.

See Also:

Oracle Database Reference for descriptions of disk group information displayed in the V\$ASM_DISKGROUP view

Figure 5 Oracle ASM Configuration Assistant Create Disk Groups Page

Disk Group Name

Redundancy

Redundancy is achieved by storing multiple copies of the data on different failure groups. Normal redundancy needs disks from at least two different failure groups, and high redundancy from at least three different failure groups.

High Normal External (None)

Select Member Disks

Show Eligible Show All

Quorum failure groups are used to store voting files in extended clusters and do not contain any user data. They require ASM compatibility of 11.2 or higher.

<input type="checkbox"/>	Disk Path	Header Status	Disk Name	Size (MB)	Failure Group	Quorum
<input type="checkbox"/>	/my_devices/diskf1	CANDIDATE		1024		<input type="checkbox"/>
<input type="checkbox"/>	/my_devices/diskf2	CANDIDATE		1024		<input type="checkbox"/>
<input type="checkbox"/>	/my_devices/diskf3	CANDIDATE		1024		<input type="checkbox"/>
<input type="checkbox"/>	/my_devices/diskl1	CANDIDATE		1024		<input type="checkbox"/>
<input type="checkbox"/>	/my_devices/diskl2	CANDIDATE		1024		<input type="checkbox"/>
<input type="checkbox"/>	/my_devices/diskl3	CANDIDATE		1024		<input type="checkbox"/>
<input type="checkbox"/>	/my_devices/diskm1	CANDIDATE		1024		<input type="checkbox"/>
<input type="checkbox"/>	/my_devices/diskm2	CANDIDATE		1024		<input type="checkbox"/>
<input type="checkbox"/>	/my_devices/diskm3	CANDIDATE		1024		<input type="checkbox"/>

Note: If you do not see the disks which you believe are available, check the Disk Discovery Path and read/write permissions on the disks. The Disk Discovery Path limits set of disks considered for discovery.

Disk Discovery Path: /my_devices

Click on the Show Advanced Options button to change the disk group attributes. Disk Group compatibility attributes may need to be modified based on the usage of disk group for different versions of databases or ASM Cluster File Systems.

On this page, you can enter a name for the disk group, select the redundancy level, change the disk discovery path to locate disks in a different directory, identify the disks to be in the disk group, enter a name for a failure group, and specify if the failure group is a quorum type.

A quorum failure group is a special type of failure group and disks in these failure groups do not contain user data and a quorum failure group is not considered when determining redundancy requirements with respect to user storage. However, a quorum failure group counts when mounting a disk group. For information about quorum failure groups, see [“Storing Oracle Cluster Registry and Voting Files in Oracle ASM Disk Groups”](#).

If Oracle ASM Filter Driver has been configured for your system, you can add Oracle ASM Filter Driver labels to disks or clear Oracle ASM Filter Driver labels from disks. For information about Oracle ASM Filter Driver, refer to [“Oracle ASM Filter Driver”](#).

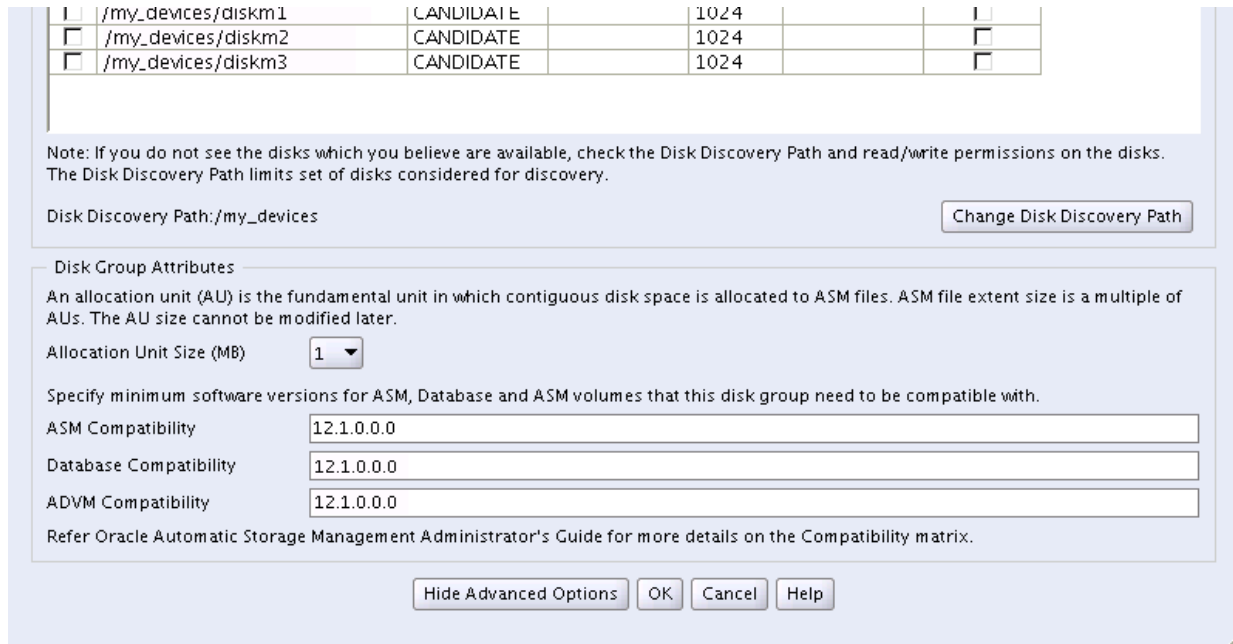
You can choose to show advanced options when creating a disk group, as shown in [Figure 6](#). The advanced options section enables you to set additional options, such as disk group compatibility settings and allocation unit (AU) size. When you are finished with the create disk group specifications, click **OK**.

For Oracle ASM 12c, the default disk group compatibility settings are 12.1 for Oracle ASM compatibility, 10.1 for database compatibility, and no value for Oracle ADVM compatibility. For information about disk group compatibility attributes, see [“Disk Group Compatibility”](#). For information about disk discovery, see [“Oracle ASM Disk Discovery”](#) and [“ASM_DISKSTRING”](#).

Note:

The disk group compatibility settings can only be advanced. You cannot revert to a lower compatibility setting after you advance the disk group compatibility settings. See [“Overview of Disk Group Compatibility”](#)

Figure 6 Oracle ASM Configuration Assistant Create Disk Groups - Advanced Options



For more information about managing disk groups, see [Administering Oracle ASM Disk Groups](#).

ASMCA Command-Line Interface

The ASMCA command-line interface provides non-GUI support for configuring Oracle ASM instances, Oracle ASM disk groups, volumes, and Oracle ACFS.

- [Running ASMCA Command-Line](#)
- [ASMCA Commands for Instances and Disk Groups](#)

Running ASMCA Command-Line

The syntax for running the ASMCA command-line tool is:

```
asmca -silent command_name [options]
```

[Table 1](#) contains the options available with the `asmca` command-line tool.

Table 1 Options for the ASMCA command-line tool

Option	Description
<code>-silent</code>	Specifies to run <code>asmca</code> in command-line mode.
<code>command_name</code>	Specifies the command to run. The command can be any of the following:

Option	Description
	<ul style="list-style-type: none"> -convertToFlexASM -configureASM -upgradeASM -configureParameter -deleteASM -createDiskGroup -addDisk -createVolume -createACFS <p>See “ASMCA Commands for Instances and Disk Groups”.</p>
<i>options</i>	<p>Specifies the options to run for a command. The options vary by command. See the individual commands described in “ASMCA Commands for Instances and Disk Groups” for the available options.</p> <p>The following list describes the options that are common for multiple commands.</p> <ul style="list-style-type: none"> • -help Displays help for running ASMCA in silent mode. • -asmsnmpPassword <i>asmsnmp_password</i> The Oracle ASM monitor user (ASMSNMP) password. This is optional and only required when creating and migrating an Oracle ASM instance. • -sysAsmPassword <i>sysasm_password</i> The SYSASM password for Oracle ASM instance. This option is required.

The following is an example of the `-help` option.

```
$ asmca -help
asmca [-silent] [-sysAsmPassword <SYS user password>] [-asmsnmpPassword <ASMSNMP password>]
{<command> <options>}
Please refer to the manual for details.
You can enter one of the following commands:
...
```

ASMCA Commands for Instances and Disk Groups

This section describes the commands that can be run with ASMCA command-line.

- [Convert to Oracle Flex ASM](#)
- [Configure an Oracle ASM Instance](#)
- [Upgrade an Oracle ASM Instance](#)
- [Configure Parameters for an Oracle ASM Instance](#)
- [Delete Oracle ASM Instances](#)
- [Create a Disk Group](#)
- [Add a Disk to a Disk Group](#)

Convert to Oracle Flex ASM

`-convertToFlexASM` converts Oracle ASM to Oracle Flex ASM

Syntax

```
asmca -silent
      -convertToFlexASM
      -asmNetworks interface_name/subnet, interface_name/subnet...
      -asmListenerPort ASM_listener_port_number
```

[Table 2](#) contains the options available with the `-convertToFlexASM` command.

Table 2 Options for the `-convertToFlexASM` command

Option	Description
<code>-asmNetworks</code>	Specifies a comma-delimited list of Oracle ASM networks. Each network is of the form <code>interface_name/subnet</code> . Specify the subnet, not the IP address for this option
<code>-asmListenerPort</code>	Specifies the Oracle ASM listener port number.

This functionality is only available in an Oracle Grid Infrastructure configuration, not an Oracle Restart configuration.

For additional options that are common to multiple commands, see [Table 1](#).

Examples

To convert Oracle ASM to Oracle Flex ASM:

Example 1 Using `asmca -silent -convertToFlexASM`

```
asmca -silent
      -convertToFlexASM
      -asmNetworks eth1/10.10.10.0
      -asmListenerPort 1521
```

Configure an Oracle ASM Instance

`-configureASM` configures or creates an Oracle ASM instance.

Syntax

```
asmca -silent
      -configureASM
      [-sysAsmPassword sysasm_password ]
      [ -asmsnmpPassword asm_monitor_password ]
      [ { -param paramname=paramvalue , ... } ]
      [ { -diskString discovery_path
          { -diskGroupName diskgroup
            { -disk disk_path [-diskName disk] |
              -diskList disk_list
                [-diskSize disk_size_MB]
                [-failuregroup failure_group]
                [-force|-noforce]
                [-quorum|-noquorum] }
          }
        [ -redundancy { HIGH | NORMAL | EXTERNAL } ] } ]
      [-au_size value]
      [-compatible.asm value ]
      [-compatible.rdbms value ]
      [-compatible.advm value ] }
```

[Table 3](#) contains the options available with the `-configureASM` command.

Table 3 Options for the `-configureASM` command

Option	Description
<code>-param paramname=paramvalue , ...</code>	Specifies a list of initialization parameters with values for the Oracle ASM instance.
<code>-diskString discovery_path</code>	Specifies the Oracle ASM discovery string for locating disks.
<code>-diskGroupName diskgroup</code>	Specifies the name of the Oracle ASM disk group to create.
<code>-disk disk_path</code>	Specifies the full path of the disk device.
<code>-diskName disk</code>	Specifies a user-supplied disk name.
<code>-diskList disk_list</code>	Specifies a comma-delimited list of disk names to be added to the disk group.
<code>-diskSize disk_size_MB</code>	Specifies the size of the disk to use for Oracle ASM storage.
<code>-failuregroup failure_group</code>	Specifies the failure group name.
<code>-force -noforce</code>	Specifies where to force the use of the disk.
<code>-quorum -noquorum</code>	Specifies a quorum or standard failure group.
<code>-redundancy { HIGH NORMAL EXTERNAL }</code>	Specifies the redundancy setting for the Oracle ASM disk group.
<code>-au_size</code>	Specifies the allocation unit size (1,2,4,8,16,32,64)
<code>-compatible.asm</code>	Specifies the attribute setting.
<code>-compatible.rdbms</code>	Specifies the attribute setting.
<code>-compatible.advm</code>	Specifies the attribute setting.

For additional options that are common to multiple commands, see [Table 1](#) .

Examples

To configure an Oracle ASM instance:

Example 2 Using `asmca -silent -configureASM`

```
asmca -silent
      -configureASM
        -diskString '/devices/disk*'
        -sysAsmPassword my_sysasm_password
        -asmsnmpPassword my_asmsnmp_passwd
```

Upgrade an Oracle ASM Instance

`-upgradeASM` upgrades an Oracle ASM instance from a previous release to the current software release.

Upgrading an Oracle ASM instance with ASMCA only updates the Oracle ASM instance software and does not configure Oracle Clusterware or the listener.

An Oracle ASM instance should be upgraded with Oracle Universal Installer (OUI). OUI automatically defaults to upgrade mode when it detects an Oracle ASM instance at a previous release level.

Syntax

```
asmca -silent
      -upgradeASM
      [-asmsnmpPassword asmsnmp_password]
```

The options available with the `-upgradeASM` command are common to multiple commands. For a description of those options, see [Table 1](#).

Examples

To upgrade an Oracle ASM instance:

Example 3 Using `asmca -silent -upgradeASM`

```
asmca -silent
      -upgradeASM
      -asmsnmpPassword my_asmsnmp_passwd
```

Configure Parameters for an Oracle ASM Instance

`-configureParameter` modifies the parameters of an Oracle ASM instance.

Syntax

```
asmca -silent
      -configureParameter
      [{-param paramname=paramvalue , ... } ]
      [-sysAsmPassword sysasm_password ]
```

[Table 4](#) contains the options available with the `-configureParameter` command.

Table 4 Options for the `-configureParameter` command

Option	Description
<code>-param <i>paramname=paramvalue</i> , ...</code>	Specifies a list of initialization parameters with values for the Oracle ASM instance.

For additional options that are common to multiple commands, see [Table 1](#).

Examples

To configure parameters for an Oracle ASM instance:

Example 4 Using `asmca -silent -configureParameter`

```
asmca -silent
      -configureParameter
      -param
      asm_power_limit=3
      -sysAsmPassword my_sysasm_password
```

Delete Oracle ASM Instances

`-deleteASM` deletes all the Oracle ASM instances that are present. The operation stops and an error is raised if there is a database using the Oracle ASM instance.

Syntax

```
asmca -silent
      -deleteASM
      [-sysAsmPassword sysasm_password ]
```

```
[-force]
[-dropDiskGroups]
```

Table 5 contains the options available with the `-deleteASM` command.

Table 5 Options for the `-deleteASM` command

Option	Description
<code>-force</code>	Forces the deletion of an Oracle ASM instance.
<code>-dropDiskGroups</code>	Drops the disk groups on this instance.

For additional options that are common to multiple commands, see Table 1 .

Examples

To delete an Oracle ASM instance:

Example 5 Using `asmca -silent -deleteASM`

```
asmca -silent
      -deleteASM
      -sysAsmPassword my_sysasm_password
      -force
```

Create a Disk Group

`-createDiskGroup` creates disk groups in an Oracle ASM instance.

Syntax

```
asmca -silent
      -createDiskGroup
      [ -diskString discovery_path ]
      { -diskGroupName diskgroup
      { -disk disk_path [-diskName disk] |
      -diskList disk_list
      [-diskSize disk_size_MB]
      [-failuregroup failure_group]
      [-force|-noforce]
      [-quorum|-noquorum] }
      [ -redundancy { HIGH | NORMAL | EXTERNAL } ] } ]
      [-au_size value]
      [-compatible.asm value ]
      [-compatible.rdbms value ]
      [-compatible.advm value ]
      [-sysAsmPassword sysasm_password ]
```

Table 6 contains the options available with the `-createDiskGroup` command.

Table 6 Options for the `-createDiskGroup` command

Option	Description
<code>-diskString <i>discovery_path</i></code>	Specifies the Oracle ASM discovery string for locating disks.
<code>-diskGroupName <i>diskgroup</i></code>	Specifies the name of the Oracle ASM disk group to create.
<code>-disk <i>disk_path</i></code>	Specifies the full path of the disk device.
<code>-diskName <i>disk</i></code>	Specifies a user-supplied disk name.

Option	Description
<code>-diskList <i>disk_list</i></code>	Specifies a comma-delimited list of disk names to be added to the disk group.
<code>-diskSize <i>disk_size_MB</i></code>	Specifies the size of the disk to use for Oracle ASM storage.
<code>-failuregroup <i>failure_group</i></code>	Specifies the failure group name.
<code>-force -noforce</code>	Specifies where to force the use of the disk.
<code>-quorum -noquorum</code>	Specifies a quorum or standard failure group.
<code>-redundancy { HIGH NORMAL EXTERNAL }</code>	Specifies the redundancy setting for the Oracle ASM disk group.
<code>-au_size</code>	Specifies the allocation unit size (1,2,4,8,16,32,64)
<code>-compatible.asm</code>	Specifies the attribute setting.
<code>-compatible.rdbms</code>	Specifies the attribute setting.
<code>-compatible.advm</code>	Specifies the attribute setting.

For additional options that are common to multiple commands, see [Table 1](#).

The default disk group compatibility settings are 11.2 for Oracle ASM compatibility, 10.1 for database compatibility, and no value for Oracle ADVM compatibility. For information about disk group compatibility attributes, see “[Disk Group Compatibility](#)”.

Examples

To create disk groups in an Oracle ASM instance:

Example 6 Using `asmca -silent -createDiskGroup`

```
$ asmca -silent -createDiskGroup
  -diskGroupName mynewdg
    -disk '/devices/diske*'
    -disk '/devices/diskk*'
  -redundancy NORMAL
  -au_size 64
  -compatible.asm '11.2.0.0.0'
  -compatible.rdbms '11.2.0.0.0'
  -compatible.advm '11.2.0.0.0'
```

DiskGroup mynewdg created successfully.

Add a Disk to a Disk Group

`-addDisk` add disks to an existing disk group in an Oracle ASM instance.

Syntax

```
asmca -silent
  -addDisk
    [ -diskString discovery_path ]
    { -diskGroupName diskgroup
      { -disk disk_path [-diskName disk] |
        -diskList disk_list
          [-diskSize disk_size_MB]
          [-failuregroup failure_group]
          [-force|-noforce]
```



```

[-quorum|-noquorum] }
[-sysAsmPassword sysasm_password ]

```

[Table 7](#) contains the options available with the `-addDisk` command.

Table 7 Options for the `-addDisk` command

Option	Description
<code>-diskString <i>discovery_path</i></code>	Specifies the Oracle ASM discovery string for locating disks.
<code>-diskGroupName <i>diskgroup</i></code>	Specifies the name of the Oracle ASM disk group to update.
<code>-diskList <i>disk_list</i></code>	Specifies a comma-delimited list of disk names to be added to the disk group.
<code>-diskSize <i>disk_size_MB</i></code>	Specifies the size of the disk to use for Oracle ASM storage.
<code>-failuregroup <i>failure_group</i></code>	Specifies the failure group name.
<code>-force -noforce</code>	Specifies where to force the use of the disk.
<code>-quorum -noquorum</code>	Specifies a quorum or standard failure group.

For additional options that are common to multiple commands, see [Table 1](#).

Examples

To add disks to an existing disk group:

Example 7 Using `asmca -silent -addDisk`

```

asmca -silent
      -addDisk
        -diskGroupName mynewdg
          -disk '/devices/disk11'
          -disk '/devices/disk12'

```

Disks added successfully to diskgroup mynewdg.

Managing Oracle ASM with ASMCMD

This chapter describes the Oracle Automatic Storage Management (Oracle ASM) Command-Line Utility (ASMCMD). This chapter contains the following topics:

- [About ASMCMD](#)
- [ASMCMD Instance Management Commands](#)
- [ASMCMD Oracle ASM Filter Driver Management Commands](#)
- [ASMCMD File Management Commands](#)
- [ASMCMD Disk Group Management Commands](#)
- [ASMCMD Template Management Commands](#)
- [ASMCMD File Access Control Commands](#)

For information about ASMCMD commands to manage volumes, refer to [Managing Oracle ADVM with ASMCMD](#).

About ASMCMD

ASMCMD is a command-line utility that you can use to manage Oracle ASM instances, disk groups, file access control for disk groups, files and directories within disk groups, templates for disk groups, and volumes.

You can run the ASMCMD utility in either interactive or noninteractive mode.

This section contains the following topics:

- [Types of ASMCMD Commands](#)
- [About Oracle ASM Files_ File Names_ Directories_ and Aliases](#)
- [Preparing to Run ASMCMD](#)
- [Running ASMCMD in Interactive Mode](#)
- [Running ASMCMD in Noninteractive Mode](#)
- [Getting Help](#)

Types of ASMCMD Commands

The types of ASMCMD commands are listed in [Table 1](#).

Table 1 Types of ASMCMD commands

Category	Commands
Oracle ASM instance management	For a list of commands, refer to “ASMCMD Instance Management Commands”
Oracle ASM Filter Driver management	For a list of commands, refer to “ASMCMD Oracle ASM Filter Driver Management Commands”
Oracle ASM file management	For a list of commands, refer to “ASMCMD File Management Commands”
Oracle ASM disk group management	For a list of commands, refer to “ASMCMD Disk Group Management Commands”
Oracle ASM template management	For a list of commands, refer to “ASMCMD Template Management Commands”
Oracle ASM file access control	For a list of commands, refer to “ASMCMD File Access Control Commands”
Oracle ADVM volume	Refer to Managing Oracle ADVM with ASMCMD

About Oracle ASM Files, File Names, Directories, and Aliases

ASMCMD works with Oracle ASM files, directories, and aliases. Before using ASMCMD, you should understand how these common computing concepts apply to the Oracle ASM environment.

This section contains the following topics:

- [System-Generated File Name or Fully Qualified File Name](#)
- [Directory](#)
- [Alias](#)
- [Absolute Path and Relative Path](#)
- [Wildcard Characters](#)

System-Generated File Name or Fully Qualified File Name

Every file created in Oracle ASM gets a system-generated file name, otherwise known as a fully qualified file name. This is similar to a complete path name in a local file system.

Oracle ASM generates file names according to the following scheme:

```
+diskGroupName/databaseName/fileType/fileTypeTag.fileNumber.incarnation
```

An example of a fully qualified file name is the following:

```
+data/orcl/CONTROLFILE/Current.256.541956473
```

In the previous fully qualified file name, `data` is the disk group name, `orcl` is the database name, `CONTROLFILE` is the file type, and so on.

Only the slash (/) is supported by ASMCMD. File Names are not case sensitive, but are case retentive. If you type a path name as lowercase, ASMCMD retains the lowercase.

For more information about Oracle ASM file names, refer to [“Fully Qualified File Name Form”](#).

Directory

As in other file systems, an Oracle ASM directory is a container for files, and an Oracle ASM directory can be part of a tree structure of other directories. The fully qualified file name represents a hierarchy of directories in which the plus sign (+) represents the root directory. In each disk group, Oracle ASM automatically creates a directory hierarchy that corresponds to the structure of the fully qualified file names in the disk group. The directories in this hierarchy are known as system-generated directories.

ASMCMD enables you to move up and down in this directory hierarchy with the `cd` (change directory) command. The `ASMCMD ls` (list directory) command lists the contents of the current directory, while the `pwd` command prints the name of the current directory.

When you start ASMCMD, the current directory is set to root (+). For an Oracle ASM instance with two disk groups, for example, `data` and `fra`, entering an `ls` command with the root directory as the current directory produces the following output:

```
ASMCMD> ls
data/
fra/
```

The following example demonstrates navigating the Oracle ASM directory tree (refer to the fully qualified file name shown previously):

```
ASMCMD> cd +data/orcl/CONTROLFILE
ASMCMD> ls
Current.256.541956473
Current.257.541956475
```

You can create your own directories as subdirectories of the system-generated directories using the `ASMCMD mkdir` command. The directories that you create can have subdirectories, and you can navigate the hierarchy of both system-generated directories and user-created directories with the `cd` command.

The following example creates the directory `mydir` under `orcl` in the disk group `data`:

```
ASMCMD> mkdir +data/orcl/mydir
```

Note:

The directory `orcl` is a system-generated directory. The contents of `data` represent the contents of disk group `data`.

If you start ASMCMD with the `-p` flag, then ASMCMD shows the current directory as part of its prompt. See [“Including the Current Directory in the ASMCMD Prompt”](#).

```
ASMCMD [+] > cd data/orcl
ASMCMD [+data/orcl] >
```

ASMCMD retains the case of the directory that you entered.

Alias

Aliases are file names that are references or pointers to system-generated file names. However, aliases are user-friendly names. Aliases are similar to symbolic links in UNIX or Linux computers. You can create aliases to simplify Oracle ASM file name

administration. You can create aliases with the `mkalias` ASMCMD command or a SQL `ALTER DISKGROUP` command.

An alias has at a minimum the disk group name as part of its complete path. You can create aliases at the disk group level or in any system-generated or user-created subdirectory. The following are examples of aliases:

```
+data/ctl1.f
+data/orcl/ctl1.f
+data/mydir/ctl1.f
```

If you run the ASMCMD `ls` (list directory) with the `-l` flag, each alias is listed with the system-generated file to which the alias refers.

```
ctl1.f => +data/orcl/CONTROLFILE/Current.256.541956473
```

For more information about aliases, refer to “[Alias Oracle ASM File Name Forms](#)”.

Absolute Path and Relative Path

When you run an ASMCMD command that accepts a file name or directory name as an argument, you can use the name as either an absolute path or a relative path.

An absolute path refers to the full path of a file or directory. An absolute path begins with a plus sign (+) followed by a disk group name, followed by subsequent directories in the directory tree. The absolute path includes directories until the file or directory of interest is reached. A complete system-generated file name, otherwise known as the fully qualified file name, is an example of an absolute path to a file.

Using an absolute path enables the command to access the file or directory regardless of where the current directory is set. The following `rm` command uses an absolute path for the file name:

```
ASMCMD [+] > rm +data/orcl/datafile/users.259.555341963
```

The following `cd` command uses an absolute path to the directory.

```
ASMCMD [+data/mydir] > cd +data/orcl/CONTROLFILE
```

A relative path includes only the part of the file name or directory name that is not part of the current directory. That is, the path to the file or directory is relative to the current directory.

In the following example, the `rm` command operates on the file `undotbs1.272.557429239`, which in this case is a relative path. ASMCMD appends the current directory to the command argument to obtain the absolute path to the file. In this example this is `+data/orcl/DATAFILE/undotbs1.272.557429239`.

```
ASMCMD [+] > cd +data
ASMCMD [+data] > cd orcl/DATAFILE
ASMCMD [+data/orcl/DATAFILE] > ls
EXAMPLE.269.555342243
SYSAUX.257.555341961
SYSTEM.256.555341961
UNDOTBS1.258.555341963
UNDOTBS1.272.557429239
USERS.259.555341963
ASMCMD [+data/orcl/DATAFILE] >
  rm undotbs1.272.557429239
```

Paths to directories can also be relative. You can go up or down the hierarchy of the current directory tree branch by providing a directory argument to the `cd` command whose path is relative to the current directory.

In addition, you can use the pseudo-directories "." and ".." rather than a directory name. The "." pseudo-directory is the current directory. The ".." pseudo-directory is the parent directory of the current directory.

The following example demonstrates how to use relative directory paths and pseudo-directories:

```
ASMCMD [+data/orcl] > cd DATAFILE
ASMCMD [+data/orcl/DATAFILE] >cd ..
ASMCMD [+data/orcl] >
```

Wildcard Characters

The wildcard characters * and % match zero or more characters anywhere within an absolute or relative path, which saves typing of the full directory or file name. The two wildcard characters behave identically. There are various ASMCMD commands that accept wildcards, such as cd, du, find, ls, lsattr, lsdg, lsdsk, lsgrp, lsusr, and rm.

If a wildcard pattern matches only one directory when using wildcard characters with cd, then cd changes the directory to that destination. If the wildcard pattern matches multiple directories, then ASMCMD does not change the directory but instead returns an error.

If you are running ASMCMD commands in noninteractive mode, then with most operating systems you must enclose the wildcard characters in quotes. For more information, refer to [“Running ASMCMD in Noninteractive Mode”](#).

[Example 1](#) illustrates the use of wildcards.

Example 1 Using wildcards with ASMCMD commands

```
ASMCMD [+] > cd +data/orcl/*FILE
ASMCMD-08005: +data/orcl/*FILE: ambiguous

ASMCMD [+] > cd +data/orcl/C*
ASMCMD [+data/orcl/CONTROLFILE] >

ASMCMD [+] > ls +fra/orcl/A%
2009_07_13/
2009_07_14/

ASMCMD [+] > ls +fra/orcl/ARCHIVELOG/2009%

+fra/orcl/ARCHIVELOG/2009_07_13/:
thread_1_seq_3.260.692103543
thread_1_seq_4.261.692108897
thread_1_seq_5.262.692125993
thread_1_seq_6.263.692140729
thread_1_seq_7.264.692143333

+fra/orcl/ARCHIVELOG/2009_07_14/:
thread_1_seq_8.271.692158265
thread_1_seq_9.272.692174597

ASMCMD [+] > ls data/orcl/*

+data/orcl/CONTROLFILE/:
Current.260.692103157

+data/orcl/DATAFILE/:
EXAMPLE.265.692103187
SYS_AUX.257.692103045
SYSTEM.256.692103045
UNDOTBS1.258.692103045
USERS.259.692103045
```

```
+data/orcl/ONLINELOG/:
group_1.261.692103161
group_2.262.692103165
group_3.263.692103169

+data/orcl/PARAMETERFILE/:
spfile.266.692103315

+data/orcl/TEMPFILE/:
TEMP.264.692103181
spfileorcl.ora
```

Preparing to Run ASMCMD

You can run the ASMCMD utility in either interactive or noninteractive mode.

Before running ASMCMD, review the items in the following list.

- Log in to the host which contains the Oracle ASM instance that you plan to administer.

You must log in as a user that has SYSASM or SYSDBA privileges through operating system authentication. The SYSASM privilege is the required connection to administer the Oracle ASM instance. See [“Authentication for Accessing Oracle ASM Instances”](#).

See Also:

Refer to the *Oracle Database Administrator's Guide* for information about operating system authentication

- To connect to the Oracle ASM instance, run ASMCMD that is located in the `bin` subdirectory of the Oracle Grid Infrastructure home (Oracle ASM home).

Connect as SYSASM, the default connection, to administer an Oracle ASM instance.

Ensure that the `ORACLE_HOME` and `ORACLE_SID` environment variables refer to the Oracle ASM instance. Depending on your operating system, you might have to set other environment variables to properly connect to the Oracle ASM instance.

Ensure that the `bin` subdirectory of your Oracle Grid Infrastructure home is in your `PATH` environment variable.

See Also:

Refer to the *Oracle Database Administrator's Guide* for more information about setting environment variables

The default value of the Oracle ASM SID for a single-instance database is `+ASM`. In Oracle Real Application Clusters environments, the default value of the Oracle ASM SID on any node is `+ASMnode#`.

- To use most of the ASMCMD commands, ensure that the Oracle ASM instance is started and the Oracle ASM disk groups are mounted.

If the Oracle ASM instance is not running, ASMCMD runs only those commands that do not require an Oracle ASM instance. The commands include `startup`,

shutdown, lsdsk, help, and exit. If you attempt to run other ASMCMD commands, an error message displays.

- You can connect to the database instance as SYSDBA by running ASMCMD that is located in the bin directory of the Oracle Database home.

Ensure that the ORACLE_HOME and ORACLE_SID environment variables refer to the database instance. Depending on your operating system, you might have to set other environment variables to properly connect to the database instance.

You must include the --privilege option to connect as SYSDBA. See “[Specifying the Type of Connection](#)”.

With this connection, there is a limited set of operations that can be run. For more information, see “[The SYSDBA Privilege for Managing Oracle ASM Components](#)”.

When administering disk groups, Oracle recommends that you run ASMCMD from the database home of the database instance that is the owner of the files in the disk group.

Running ASMCMD in Interactive Mode

The interactive mode of the ASMCMD utility provides a shell-like environment where you are prompted to enter ASMCMD commands.

This section contains the following topics:

- [Syntax for Starting ASMCMD](#)
- [Running ASMCMD without Any Options](#)
- [Specifying the Type of Connection](#)
- [Specifying the Verbose Mode](#)
- [Including the Current Directory in the ASMCMD Prompt](#)
- [Displaying the ASMCMD Version Number](#)

Syntax for Starting ASMCMD

The syntax for starting ASMCMD in interactive mode is:

```
asmcmd [-V]
asmcmd [--nocp] [-v {errors|warnings|normal|info|debug}]
           [--privilege connection_type ] [-p]
```

[Table 2](#) summarizes the ASMCMD options.

Table 2 ASMCMD interactive options

Option	Description
-V	Displays the version of ASMCMD and then exits.
--nocp	Disables connection pooling. For information about connection pooling, refer to <i>Oracle Database Administrator's Guide</i> .
-v <i>display_level</i>	Displays additional information with some commands to help users diagnose problems and writes to a message file when logging is required. <i>normal</i> is the default if the display level is not specified.

Option	Description
<code>--privilege connection_type</code>	Specifies the privilege to connect as when accessing an Oracle ASM or database instance. Can be either <code>SYSASM</code> or <code>SYSDBA</code> . The default is <code>SYSASM</code> and is used when administering the Oracle ASM instance.
<code>-p</code>	Displays the current directory in the prompt.

ASMCMD can be started with multiple options. For example:

```
asmcmd -p -v info
```

For the majority of the examples in this chapter, ASMCMD was started with the `-p` option.

Running ASMCMD without Any Options

To run ASMCMD in interactive mode without any options:

1. Enter the following at the operating system command prompt:

```
asmcmd
```

Oracle displays an ASMCMD command prompt as follows:

```
ASMCMD>
```

2. Enter an ASMCMD command and press `Enter`. The command runs and displays its output, if any, and then ASMCMD prompts for the next command.
3. Continue entering ASMCMD commands until you have completed the tasks.
4. Enter the `exit` or `quit` command to exit ASMCMD.

Specifying the Type of Connection

You can specify the `--privilege` option to choose the type of connection, either `SYSASM` or `SYSDBA`. The default value is `SYSASM` and is used when administering an Oracle ASM instance. Connect as `SYSDBA` when connecting to the database instance.

For example:

```
$ asmcmd --privilege sysasm
```

Specifying the Verbose Mode

You can specify the `-v` option with the `asmcmd` command to display additional information with some commands to help users diagnose problems as shown in the following example:

```
$ asmcmd -v debug
```

When there is a message that must be logged during `asmcmd` operations, the message is written to the `alert.log` file or the `trace.trc` file.

The `alert.log` file is created or updated when `asmcmd` is started with the `-v errors`, `-v warning`, or `-v normal` display level. The `trace.trc` file is created or updated when `asmcmd` is started with the `-v info` or `-v debug` display level.

By default, the `alert.log` file is created in the `$ORACLE_HOME/log/diag/asmcmd/user_username/hostname/alert/` directory. By default, the `trace.trc` file is created in the `$ORACLE_HOME/log/diag/asmcmd/user_username/hostname/trace/` directory.

Under certain circumstances, `$ORACLE_BASE` and `$ORACLE_HOME` can be set to override the default locations of the `alert.log` and `trace.trc` files.

Including the Current Directory in the ASMCMD Prompt

You can specify the `-p` option with the `asmcmd` command to include the current directory in the ASMCMD prompt as shown in the following example:

```
$ asmcmd -p
ASMCMD [+] > cd data
ASMCMD [+data] >
```

Displaying the ASMCMD Version Number

You can specify the `-V` option when starting `asmcmd` to display the `asmcmd` version number. After displaying the version number, `asmcmd` immediately exits.

For example:

```
$ asmcmd -V
asmcmd version 11.2.0.3.0
$
```

Running ASMCMD in Noninteractive Mode

In noninteractive mode, you run a single ASMCMD command by including the command and command options on the command line when invoking ASMCMD. ASMCMD runs the command, generates output if any, and then exits. The noninteractive mode is especially useful for running scripts.

On most operating systems, wildcard characters must be enclosed in quotes when running ASMCMD commands in noninteractive mode.

To run ASMCMD in noninteractive mode where *command* is any valid ASMCMD command and *options* is a list of command options, at the command prompt enter the following:

```
asmcmd command options
```

In noninteractive mode, ASMCMD returns the codes listed in [Table 3](#).

Table 3 ASMCMD return codes

Type	Return Code	Description
General	0	No issues for the command.
General	1	Internal error.
General	255 or -1	External user error as returned by a command.
lsdsk	0	Results include member disks only.
lsdsk	1	Results include candidate disks only.
lsdsk	2	Results include both member and candidate disks.

[Example 2](#) shows how to run ASMCMD in the noninteractive mode. The first command runs the `ls` command to list the disk groups for the Oracle ASM instance. The second command redirects the output of the `lsod` command to the `my_lsod_test` file. The third command runs `lsdsk` using a pattern with a wildcard character to list specific disks in the `data` disk group. Note that wildcard characters must be enclosed in quotes when running ASMCMD in noninteractive mode on most operating systems.

Example 3 raises an error with an incorrect disk group name and the return code equal (255) is displayed.

Example 4 shows an example of ASMCMD commands run in noninteractive mode inside a script.

Example 2 Running ASMCMD commands in noninteractive mode

```
$ asmcmd ls -l
State   Type   Rebal  Name
MOUNTED NORMAL N      DATA/
MOUNTED NORMAL N      FRA/

$ asmcmd lsod --suppressheader -G data > my_lsod_test

$ asmcmd lsdsk -G data '/devices/diska*'
Path
/devices/diska1
/devices/diska2
/devices/diska3
```

Example 3 Displaying a return code when running ASMCMD in noninteractive mode

```
$ asmcmd ls -l dat
ASMCMD-08001: diskgroup 'dat' does not exist or is not mounted

$ echo $?
255
```

Example 4 Running ASMCMD commands in a script

```
#!/bin/sh
for ((i = 1; i <=3; i++))
do
    asmcmd lsdsk -G data '/devices/diska'$i
done

$ ./asmcmd_test_script
Path
/devices/diska1
Path
/devices/diska2
Path
/devices/diska3
```

Getting Help

Type `help` at the ASMCMD prompt or as a command in noninteractive mode to view general information about ASMCMD and a list of available ASMCMD commands.

You can type `help command` to display help text for a specific command, including usage information about how to run the command with its options.

The following is an example of the use of the `help` command.

Example 5 Displaying ASMCMD help text

```
ASMCMD [+] > help startup
startup [--nomount] [--restrict] [--pfile <pfile.ora>]

Start the ASM instance.

[--nomount]           specifies the nomount option.
[--restrict]          start the instance in restricted mode.
[--pfile <pfile.ora>] specifies the location of the file.
```

ASMCMD Instance Management Commands

This section describes the ASMCMD Oracle ASM instance management commands.

Some commands in this section affect the Grid Plug and Play (GPnP) profile, which is a resource in a clustered configuration. In an Oracle Restart configuration, the profile is actually located in a resource attribute, not the Grid Plug and Play (GPnP) profile. However, the functionality of the commands is the same for both configurations.

See Also:

Oracle Grid Infrastructure Installation Guide for your operating system for information about installing and configuring Oracle Grid Infrastructure

[page 10-11](#) provides a summary of the Oracle ASM instance management commands.

Command	Description
dsget	Retrieves the discovery diskstring value that is used by the Oracle ASM instance and its clients.
dsset	Sets the disk discovery diskstring value that is used by the Oracle ASM instance and its clients.
lsct	Lists information about current Oracle ASM clients.
lsop	Lists the current operations on a disk group or Oracle ASM instance.
lspwusr	Lists the users from an Oracle ASM password file.
orapwusr	Adds, drops, or changes an Oracle ASM password user.
pwcopy	Copies a password file to the specified location.
pwcreate	Creates a password file at the specified location.
pwdelete	Deletes a password file at the specified location.
pwget	Returns the location of the password file.
pwmove	Moves the location of the password file.
pwset	Sets the location of the password file.
showclustermode	Displays the current mode of the Oracle ASM cluster.
showclusterstate	Displays the current state of the cluster.
showpatches	Lists the patches applied to the Oracle Grid Infrastructure home.
showversion	Displays the Oracle ASM cluster release and software patch levels.
shutdown	Shuts down an Oracle ASM instance.
spbackup	Backs up an Oracle ASM SPFILE.
spcopy	Copies an Oracle ASM SPFILE.
spget	Retrieves the location of the Oracle ASM SPFILE.
spmmove	Moves an Oracle ASM SPFILE.

Command	Description
spset	Sets the location of the Oracle ASM SPFILE.
startup	Starts up an Oracle ASM instance.

dsget

Purpose

Retrieves the discovery diskstring value that is used by the Oracle ASM instance and its clients.

Syntax and Description

```
dsget [ --normal | --parameter | --profile [-f] ]
```

The syntax options for the `dsget` command are described in [Table 5](#).

Table 5 Options for the `dsget` command

Option	Description
<code>--normal</code>	Retrieves the discovery string from the Grid Plug and Play (GPnP) profile and the one that is set in the Oracle ASM instance. It returns one row each for the profile and parameter setting. This is the default setting.
<code>--parameter</code>	Retrieves the <code>ASM_DISKSTRING</code> parameter setting of the Oracle ASM instance.
<code>--profile [-f]</code>	Retrieves the discovery string from the GPnP profile. If <code>-f</code> is specified with <code>--profile</code> , <code>dsget</code> retrieves the discovery string from the local GPnP profile.

Example

The following example uses `dsget` to retrieve the current discovery diskstring value from the GPnP profile and the `ASM_DISKSTRING` parameter.

Example 6 Using the ASMCMD `dsget` command

```
ASMCMD [+] > dsget
profile: /devices1/disk*
parameter: /devices2/disk*
```

dsset

Purpose

Sets the discovery diskstring value that is used by the Oracle ASM instance and its clients.

The specified diskstring must be valid for existing mounted disk groups. The updated value takes effect immediately.

Syntax and Description

```
dsset [ --normal | --parameter | --profile [-f] ] diskstring
```

The syntax options for the `dsset` command are described in [Table 6](#).

Table 6 Options for the dsset command

Option	Description
<code>--normal</code>	Sets the discovery string in the Grid Plug and Play (GPnP) profile and in the Oracle ASM instance. The update occurs after the Oracle ASM instance has successfully validated that the specified discovery string has discovered all the necessary disk groups and voting files. This command fails if the instance is not using a server parameter file (SPFILE). This is the default setting.
<code>--parameter</code>	Specifies that the diskstring is updated in memory after validating that the discovery diskstring discovers all the current mounted disk groups and voting files. The diskstring is not persistently recorded in either the SPFILE or the GPnP profile.
<code>--profile [-f]</code>	Specifies the discovery diskstring that is pushed to the GPnP profile without any validation by the Oracle ASM instance, ensuring that the instance can discover all the required disk groups. The update is guaranteed to be propagated to all the nodes that are part of the cluster. If <code>-f</code> is specified with <code>--profile</code> , the specified diskstring is pushed to the local GPnP profile without any synchronization with other nodes in the cluster. This command option updates only the local profile file. This option should only be used for recovery. The command fails if the Oracle Clusterware stack is running.
<i>diskstring</i>	Specifies the value for the discovery diskstring.

For information about disk discovery and the discovery diskstring, see “[Oracle ASM Disk Discovery](#)”.

Example

The following example uses `dsset` to set the current value of the discovery diskstring in the GPnP profile.

Example 7 Using the ASMCMD dsset command

```
ASMCMD [+] > dsset /devices1/disk*,/devices2/disk*
```

lsct

Purpose

Lists information about current Oracle ASM clients from the `V$ASM_CLIENT` view. A client, such as Oracle Database or Oracle ASM Dynamic Volume Manager (Oracle ADVM), uses disk groups that are managed by the Oracle ASM instance to which ASMCMD is currently connected.

Syntax and Description

```
lsct [--suppressheader] [-g] diskgroup
```

[Table 7](#) lists the options for the `lsct` command.

Table 7 Options for the *lsct* command

Option	Description
(none)	Displays information about current clients from the V\$ASM_CLIENT view.
-g	Selects from the GV\$ASM_CLIENT view. GV\$ASM_CLIENT.INST_ID is included in the output.
--suppressheader	Suppresses column headings.
<i>diskgroup</i>	Specifies the disk group.

Client information is only listed for the specified disk group.

Example

The following example displays information about the clients that are accessing the data disk group.

Example 8 Using the ASMCMD *lsct* command

```
ASMCMD [+] > lsct data
DB_Name Status Software_Version Compatible_version Instance_Name
Disk_Group
+ASM CONNECTED 12.1.0.0.1 12.1.0.0.1 +ASM DATA
asmvol CONNECTED 12.1.0.0.1 12.1.0.0.1 +ASM DATA
orcl CONNECTED 12.1.0.0.1 12.0.0.0.0 orcl DATA
```

lsop

Purpose

Lists the current operations on a disk group in an Oracle ASM instance.

Syntax and Description

```
lsop
```

lsop displays information from the V\$ASM_OPERATION view.

Example

The following are examples of the *lsop* command. The examples list operations on the disk groups of the current Oracle ASM instance.

Example 9 Using the ASMCMD *lsop* command

```
ASMCMD [+] > lsop
Group_Name Dsk_Num State Power
DATA REBAL WAIT 2

ASMCMD [+] > lsop
Group_Name Dsk_Num State Power
FRA REBAL REAP 3
```

lspwusr

Purpose

List the users from the local Oracle ASM password file.

Syntax and Description

```
lspwusr [--suppressheader]
```

Table 8 lists the options for the `lspwusr` command.

Table 8 Options for the `lspwusr` command

Option	Description
<code>--suppressheader</code>	Suppresses column headers from the output.

Examples

The following is an example of the `lspwusr` example. The example lists the current users in the local Oracle ASM password file.

Example 10 Using the ASMCMD `lspwusr` command

```
ASMCMD [+] > lspwusr
Username sysdba sysoper sysasm
        SYS   TRUE   TRUE   TRUE
        ASMSNMP TRUE  FALSE FALSE
```

orapwusr

Purpose

Add, drop, or modify an Oracle ASM password file user.

Syntax and Description

```
orapwusr { --add | --modify | --delete | grant {sysasm|sysdba|sysoper} |
          --revoke {sysasm|sysdba|sysoper} } user
```

Table 9 lists the options for the `orapwusr` command.

Table 9 Options for the `orapwusr` command

Option	Description
<code>--add</code>	Adds a user to the password file. Also prompts for a password.
<code>--modify</code>	Changes the password for the specified user.
<code>--delete</code>	Drops a user from the password file.
<code>--grant role</code>	Sets the role for the user. The options are <code>sysasm</code> , <code>sysdba</code> , and <code>sysoper</code> .
<code>--revoke role</code>	Removes the role for the user. The options are <code>sysasm</code> , <code>sysdba</code> , and <code>sysoper</code> .
<code>user</code>	Name of the user to add, drop, or modify.

`orapwusr` attempts to update passwords on all nodes in a cluster. This command requires the SYSASM privilege to run. A user logged in as SYSDBA cannot change its password using this command.

Examples

The following is an example of the `orapwusr` command. This example adds the `hruser` to the Oracle ASM password file.

Example 11 Using the ASMCMD orapwusr command

```
ASMCMD [+] > orapwusr --add hruser
```

pwcopy

Purpose

Copies an Oracle ASM or database instance password file to the specified location.

Syntax and Description

```
pwcopy [--asm | --dbunique string] source destination
```

Table 10 lists the options for the pwcopy command.

Table 10 Options for the pwcopy command

Option	Description
--asm	The --asm option associates the password file with the Oracle ASM instance that ASMCMD is logged into.
--dbunique <i>string</i>	The --dbunique <i>string</i> option identifies the database unique name associated with the password file.
<i>source</i>	The <i>source</i> value identifies the location where the existing password file is located.
<i>destination</i>	The <i>destination</i> value identifies the location where you want to copy the password file.

pwcopy copies a password file from one disk group to another, from the operating system to a disk group, or from a disk group to the operating system. The compatible.asm disk group attribute must be set to 12.1 or higher for the disk group where the password is to be copied.

Either --asm or --dbunique is required to identify a CRSD resource. When either --asm or --dbunique is included in the pwcopy command, the target file is set to the current password file.

The SYSASM or SYSDBA privilege is required to manage the Oracle ASM and database password files.

Example

The following example copies an Oracle ASM password file in one disk group to a different disk group. Because the pwcopy command includes the --asm option, the target file (+fra/orapwasm_new) is set to the current password file.

Example 12 Using the ASMCMD pwcopy command

```
ASMCMD [+] > pwcopy --asm +DATA/orapwasm +FRA/orapwasm_new
copying +DATA/orapwasm -> +FRA/orapwasm_new
```

pwcreate

Purpose

Creates an Oracle ASM or database instance password file at the specified location.

Syntax and Description

```
pwcreate { --asm | --dbuniqueusername string } file_path sys_password
```

[Table 11](#) lists the options for the `pwcreate` command.

Table 11 Options for the `pwcreate` command

Option	Description
<code>--asm</code>	The <code>--asm</code> option associates the password file with the Oracle ASM instance that ASMCMD is logged into.
<code>--dbuniqueusername <i>string</i></code>	The <code>--dbuniqueusername <i>string</i></code> option identifies the database unique name associated with the password file.
<i>file_path</i>	The <i>file_path</i> value identifies the location where the password file is created.
<i>sys_password</i>	The <i>sys_password</i> value identifies the initial SYS password.

`pwcreate` creates a password file in the disk group specified by *file_path* with an initial SYS password identified by *sys_password*.

Either `--asm` or `--dbuniqueusername` is required. The `compatible.asm` disk group attribute must be set to 12.1 or higher for the disk group where the password is to be located.

The SYSASM or SYSDBA privilege is required to manage the Oracle ASM and database password files.

For additional information, refer to [“Managing a Shared Password File in a Disk Group”](#).

Example

The following example creates an Oracle ASM password file in an Oracle ASM disk group.

Example 13 Using the ASMCMD `pwcreate` command

```
ASMCMD [+] > pwcreate --asm '+DATA/orapwasm' 'welcome'
```

pwdelete

Purpose

Deletes an Oracle ASM or database instance password file.

Syntax and Description

```
pwdelete { --asm | --dbuniqueusername string | file_path }
```

[Table 12](#) lists the options for the `pwdelete` command.

Table 12 Options for the `pwdelete` command

Option	Description
<code>--asm</code>	The <code>--asm</code> option associates the password file with the Oracle ASM instance that ASMCMD is logged into.

Option	Description
<code>--dbuniquefilename <i>string</i></code>	The <code>--dbuniquefilename <i>string</i></code> option identifies the database unique name associated with the password file.
<code><i>file_path</i></code>	The <code><i>file_path</i></code> value identifies the location where the password file is located.

`pwddelete` deletes the specified password file. Either `--asm` or `--dbuniquefilename` is required to identify a CRSD resource and to remove the password location from the CRSD resource.

The `SYSASM` or `SYSDBA` privilege is required to manage the Oracle ASM and database password files.

Example

The following example deletes the specified password file from a disk group.

Example 14 Using the ASMCMD pwddelete command

```
ASMCMD [+] > pwddelete +FRA/orapwasm_bak
```

pwget

Purpose

Returns the location of the password file for the Oracle ASM or database instance.

Syntax and Description

```
pwget { --asm | --dbuniquefilename string }
```

[Table 13](#) lists the options for the `pwget` command.

Table 13 Options for the pwget command

Option	Description
<code>--asm</code>	The <code>--asm</code> option associates the password file with the Oracle ASM instance that ASMCMD is logged into.
<code>--dbuniquefilename <i>string</i></code>	The <code>--dbuniquefilename <i>string</i></code> option identifies the database unique name associated with the password file.

`pwget` returns the location of the password file for the Oracle ASM instance identified by `--asm` or the database instance identified by `--dbuniquefilename`.

The `SYSASM` or `SYSDBA` privilege is required to manage the Oracle ASM and database password files.

Example

The following example returns the location of the Oracle ASM password file.

Example 15 Using the ASMCMD pwget command

```
ASMCMD [+] > pwget --asm
+DATA/orapwasm
```

pwmove

Purpose

Moves an Oracle ASM or database instance password file to the specified location.

Syntax and Description

```
pwmove { --asm | --dbuniquefilename string } source destination
```

[Table 14](#) lists the options for the `pwmove` command.

Table 14 Options for the `pwmove` command

Option	Description
<code>--asm</code>	The <code>--asm</code> option associates the password file with the Oracle ASM instance that ASMCMD is logged into.
<code>--dbuniquefilename <i>string</i></code>	The <code>--dbuniquefilename <i>string</i></code> option identifies the database unique name associated with the password file.
<i>source</i>	The <i>source</i> value identifies the location where the existing password file is located.
<i>destination</i>	The <i>destination</i> value identifies the location where you want to move the password file.

`pwmove` moves a password file from one disk group to another, from the operating system to a disk group, or from a disk group to the operating system.

Either `--asm` or `--dbuniquefilename` is required to identify a CRSD resource. The `compatible.asm` disk group attribute must be set to 12.1 or higher for the disk group where the password is to be moved.

The `SYSASM` or `SYSDBA` privilege is required to manage the Oracle ASM and database password files.

Example

The following example moves a password file from one disk group to another disk group.

Example 16 Using the ASMCMD `pwmove` command

```
ASMCMD [+] > pwmove --asm +FRA/orapwasm_bak +DATA/orapwasm
moving +FRA/orapwasm_bak -> +DATA/orapwasm
```

pwset

Purpose

Sets the location of the password file for an Oracle ASM or database instance.

Syntax and Description

```
pwset { --asm | --dbuniquefilename string } file_path
```

[Table 15](#) lists the options for the `pwset` command.

Table 15 Options for the pwset command

Option	Description
--asm	The --asm option associates the password file with the Oracle ASM instance that ASMCMD is logged into.
--dbunique <i>string</i>	The --dbunique <i>string</i> option identifies the database unique name associated with the password file.
<i>file_path</i>	The <i>file_path</i> value identifies the location where the password file is located.

pwset sets the location of the password file for an Oracle ASM or database instance to the value specified by *file_path*. Either --dbunique or --asm is required to identify a CRS resource.

The SYSASM or SYSDBA privilege is required to manage the Oracle ASM and database password files.

Example

The following example sets the location of the Oracle ASM password file in a disk group.

Example 17 Using the ASMCMD pwset command

```
ASMCMD [+] > pwset --asm +DATA/orapwasm
```

showclustermode

Purpose

Displays the current mode of the Oracle ASM cluster.

Syntax and Description

```
showclustermode
```

showclustermode displays the mode that the Oracle ASM cluster is currently in. The possible return values are **ASM cluster : Flex mode enabled** or **ASM cluster : Flex mode disabled**.

Example

The following example shows the use of the showclustermode command.

Example 18 Using the ASMCMD showclustermode command

```
ASMCMD [+] > showclustermode
ASM cluster : Flex mode disabled
```

showclusterstate

Purpose

Displays the current state of the cluster.

Syntax and Description

```
showclusterstate
```

`showclusterstate` displays the state that the Oracle ASM cluster is currently in. The possible values returned are **normal**, **in-upgrade**, or **in-rollingpatch** mode.

Example

This example shows the use of the `showclusterstate` command.

Example 19 Using the ASMCMD showclusterstate command

```
ASMCMD [+] > showclusterstate
```

showpatches

Purpose

Lists the patches applied on the Oracle Grid Infrastructure home.

Syntax and Description

```
showpatches
```

`showpatches` lists the patches that have been applied to the Oracle Grid Infrastructure home.

Example

This example shows the use of the `showpatches` command.

Example 20 Using the ASMCMD showpatches command

```
ASMCMD [+] > showpatches
-----
List of Patches
=====
```

showversion

Purpose

Displays the patch levels of the Oracle ASM cluster release and software.

Syntax and Description

```
showversion [--releasepatch] [--softwarepatch]
```

[Table 16](#) lists the options for the `showversion` command.

Table 16 Options for the showversion command

Option	Description
<code>--releasepatch</code>	Displays the cluster level patch version.
<code>--softwarepatch</code>	Displays the patch level on the local node.

`showversion` displays the Oracle ASM cluster release and software patch levels. The release and software patch options may differ depending whether the Oracle ASM or Oracle Grid Infrastructure home is being patched.

Example

This example shows the use of the `showversion` command.

Example 21 Using the ASMCMD showversion command

```
ASMCMD [+] > showversion --softwarepatch
ASM version      : 12.1.0.1.0
Software patchlevel : 0

ASMCMD [+] > showversion --releasepatch
ASM version      : 12.1.0.1.0
```

shutdown

Purpose

Shuts down an Oracle ASM instance.

Syntax and Description

```
shutdown [--normal | --abort|--immediate ]
```

[Table 17](#) lists the options for the shutdown command.

Table 17 Options for the shutdown command

Option	Description
--normal	Shut down normal.
--abort	Shut down aborting all existing operations.
--immediate	Shut down immediately.

The default action is a normal shutdown if an option is not specified.

Oracle strongly recommends that you shut down all database instances that use the Oracle ASM instance and dismount all file systems mounted on Oracle ASM Dynamic Volume Manager (Oracle ADVM) volumes before attempting to shut down the Oracle ASM instance with the `abort` (`--abort`) option.

For more information about shutting down an Oracle ASM instance, see [“About Shutting Down an Oracle ASM Instance”](#).

Example

The following are examples of the `shutdown` command. The first example performs a shut down of the Oracle ASM instance with normal action. The second example performs a shut down with immediate action. The third example performs a shut down that aborts all existing operations.

Example 22 Using the ASMCMD shutdown command

```
ASMCMD [+] > shutdown --normal

ASMCMD [+] > shutdown --immediate

ASMCMD [+] > shutdown --abort
```


spbackup

Purpose

Backs up an Oracle ASM SPFILE to a backup file.

Syntax and Description

```
spbackup source destination
```

[Table 18](#) lists the options for the `spbackup` command.

Table 18 Options for the `spbackup` command

Option	Description
<i>source</i>	Specifies the source file name.
<i>destination</i>	Specifies the destination file.

`spbackup` should be used when you want to make single or multiple backups of an SPFILE in the same or a different disk group without creating an SPFILE in the target disk group.

Note the following about the use of `spbackup`:

- `spbackup` can back up an Oracle ASM SPFILE from a disk group to a disk group or to an operating system file.
- `spbackup` can back up an Oracle ASM SPFILE from an operating system file to a disk group.
- `spbackup` can back up an Oracle ASM SPFILE when the SPFILE is being used by an open Oracle ASM instance.
- `spbackup` can make multiple backups of an Oracle ASM SPFILE in the same disk group.

`spbackup` does not affect the GPnP profile. The backup file that is created is not a special file type and is not identified as an SPFILE. This backup file cannot be copied with `spcopy`. To copy this backup file to and from a disk group, use the ASMCMD `cp` command.

To make a copy of a backup file in a disk group that is identified as an SPFILE file:

1. Use the ASMCMD `cp` command to copy the backup file from the disk group to an operating system file. See "[cp](#)".
2. Use the ASMCMD `spcopy` command to copy the operating system file to a disk group. See "[spcopy](#)".

Example

The following are examples of the `spbackup` command. The first example backs up the SPFILE in the `data` disk group. The second example backs up the SPFILE from the `data` disk group to the `fra` disk group.

Example 23 Using the ASMCMD *spbackup* command

```
ASMCMD> spbackup +DATA/asm/asmparameterfile/registry.253.721810181
+DATA/spfileBackASM.bak

ASMCMD> spbackup +DATA/asm/asmparameterfile/registry.253.721810181
+FRA/spfileBackASM.bak
```

spcopy

Purpose

Copies an Oracle ASM SPFILE from the source location to an SPFILE in the destination location.

Syntax and Description

```
spcopy [-u] source destination
```

[Table 19](#) lists the options for the *spcopy* command.

Table 19 Options for the *spcopy* command

Option	Description
-u	Updates the Grid Plug and Play (GPnP) profile.
<i>source</i>	Specifies the source file name.
<i>destination</i>	Specifies the destination.

Note the following about the use of *spcopy*:

- *spcopy* can copy an Oracle ASM SPFILE from a disk group to a different disk group or to an operating system file.
- *spcopy* can copy an Oracle ASM SPFILE from an operating system file to a disk group.
- *spcopy* can copy an Oracle ASM SPFILE when the SPFILE is being used by an open Oracle ASM instance.
- *spcopy* cannot make multiple copies of an Oracle ASM SPFILE in the same disk group. You can use *spbackup* for that purpose.

To update the GPnP profile, include the *-u* option with *spcopy*. You can also use *spset* to update the GPnP profile if *spcopy* is run without the *-u* option. See [“spset”](#). For information about copying and moving an Oracle ASM instance initialization parameter file after upgrading, see [“About Backing Up_ Copying_ and Moving an Oracle ASM Initialization Parameter File”](#).

After copying the SPFILE and updating the GPnP profile, you must restart the instance with the SPFILE in the new location to use that SPFILE. When the Oracle ASM instance is running with the SPFILE in the new location, you can remove the source SPFILE.

To copy an Oracle ASM SPFILE into a disk group using *spcopy*, the COMPATIBLE.ASM attribute must be set to 11.2 or greater in the target disk group.

See Also:

The `CREATE SPFILE` SQL statement in the *Oracle Database SQL Language Reference* for information about creating a server parameter file

Example

The following are examples of the `spcopy` command. The first example copies the Oracle ASM SPFILE from the data disk group to the `fra` disk group. The second example copies the Oracle ASM SPFILE from the data disk group to an operating system location. The third example copies an Oracle ASM SPFILE from an operating system location to the data disk group and updates the GPnP profile with the `-u` option.

Example 24 Using the ASMCMD `spcopy` command

```
ASMCMD> spcopy +DATA/asm/asmparameterfile/registry.253.721810181
             +FRA/spfileCopyASM.ora

ASMCMD> spcopy +DATA/asm/asmparameterfile/registry.253.721810181
             $ORACLE_HOME/dbs/spfileCopyASM.ora

ASMCMD> spcopy -u /oracle/product/11.2.0/grid/dbs/spfileTestASM.ora
             +DATA/ASM/spfileCopyASM.ora
```

spget**Purpose**

Retrieves the location of the Oracle ASM SPFILE from the Grid Plug and Play (GPnP) profile.

Syntax and Description

```
spget
```

The location retrieved by `spget` is the location in the GPnP profile, but not always the location of the SPFILE currently used. For example, the location could have been recently updated by `spset` or `spcopy` with the `-u` option on an Oracle ASM instance that has not been restarted. After the next restart of the Oracle ASM, this location points to the Oracle ASM SPFILE currently being used.

Example

The following is an example of the `spget` command that retrieves and displays the location of the SPFILE from the GPnP profile.

Example 25 Using the ASMCMD `spget` command

```
ASMCMD [+] > spget
+DATA/ASM/ASMPARAMETERFILE/registry.253.813507611
```

spmove**Purpose**

Moves an Oracle ASM SPFILE from source to destination and automatically updates the GPnP profile.

Syntax and Description

`spmove source destination`

Table 20 lists the options for the `spmove` command.

Table 20 Options for the `spmove` command

Option	Description
<code>source</code>	Specifies the source file.
<code>destination</code>	Specifies the destination file.

Note the following about the use of `spmove`:

- `spmove` can move an Oracle ASM SPFILE when the open instance is using a PFILE or a different SPFILE. After moving the SPFILE, you must restart the instance with the SPFILE in the new location to use that SPFILE.
- `spmove` cannot move an Oracle ASM SPFILE when the SPFILE is being used by an open Oracle ASM instance.

For information about copying and moving an Oracle ASM instance initialization parameter file after upgrading, see “[About Backing Up_ Copying_ and Moving an Oracle ASM Initialization Parameter File](#)”.

To use `spmove` to move an Oracle ASM SPFILE into a disk group, the disk group attribute `COMPATIBLE .ASM` must be set to 11 . 2 or greater.

Example

The following are examples of the `spmove` command. The first example moves an Oracle ASM SPFILE from the `data` disk group to an operating system location. The second example moves an SPFILE from an operating system location to the `data` disk group.

Example 26 Using the ASMCMD `spmove` command

```
ASMCMD> spmove +DATA/spfileASM.ora
           /oracle/product/11.2.0/grid/dbs/spfileMoveASM.ora

ASMCMD> spmove /oracle/product/11.2.0/grid/dbs/spfile+ASM.ora
           +DATA/ASM/spfileMoveASM.ora
```

spset

Purpose

Sets the location of the Oracle ASM SPFILE in the Grid Plug and Play (GPnP) profile.

Syntax and Description

`spset location`

Table 21 lists the options for the `spset` command.

Table 21 Options for the spset command

Option	Description
<i>location</i>	Specifies the location of the Oracle ASM SPFILE. The location is the full path to the SPFILE.

Example

The following is an example of the spset command that sets the location of the Oracle ASM SPFILE command in the data disk group.

Example 27 Using the ASMCMD spset command

```
ASMCMD> spset +DATA/asm/asmparameterfile/asmspfile.ora
```

startup

Purpose

Starts up an Oracle ASM instance.

Syntax and Description

```
startup [--nomount] [--restrict] [ --pfile pfile ]
```

[Table 22](#) lists the options for the startup command.

Table 22 Options for the startup command

Option	Description
--nomount	Specifies no mount operation.
--restrict	Specifies restricted mode.
--pfile <i>pfile</i>	Oracle ASM initialization parameter file.

The default action is a startup that mounts disk groups and enables Oracle ASM Dynamic Volume Manager (Oracle ADVM) volumes. For information about disk groups that are mounted at startup time, see [“About Mounting Disk Groups at Startup”](#).

For more information about starting up an Oracle ASM instance, see [“About Starting Up an Oracle ASM Instance”](#).

Example

The following is an example of the startup command that starts the Oracle ASM instance without mounting disk groups and uses the asm_init.ora initialization parameter file.

Example 28 Using the ASMCMD startup command

```
ASMCMD> startup --nomount --pfile asm_init.ora
```

ASMCMD Oracle ASM Filter Driver Management Commands

This section describes the ASMCMD Oracle ASM Filter Driver management commands.

See Also:

Oracle Grid Infrastructure Installation Guide for your operating system for information about installing and configuring Oracle Grid Infrastructure

[page 10-28](#) provides a summary of the Oracle ASM Filter Driver management commands.

Command	Description
afd_configure	Configures Oracle ASM Filter Driver.
afd_deconfigure	Deconfigures Oracle ASM Filter Driver.
afd_dsget	Retrieves the Oracle ASM Filter Driver diskstring value.
afd_dsset	Sets the Oracle ASM Filter Driver diskstring value.
afd_filter	Sets the Oracle ASM Filter Driver mode on a given disk path.
afd_label	Sets an Oracle ASM Filter Driver label to a disk.
afd_lsdisk	Lists Oracle ASM Filter Driver disks.
afd_scan	Scans for Oracle ASM Filter Driver disks.
afd_state	Returns the state of Oracle ASM Filter Driver.
afd_unlabel	Clears an existing Oracle ASM Filter Driver label.

afd_configure

Purpose

Configures Oracle ASM Filter Driver.

Syntax and Description

```
# asmcmd afd_configure
```

The `afd_configure` command must be run noninteractively as a `root` user. Before running the command on a node, the Oracle Clusterware stack must be shut down on that node. After the `afd_configure` command has been run, restart Oracle Clusterware on each node.

For information about Oracle ASM Filter Driver, refer to "[Oracle ASM Filter Driver](#)".

See Also:

Oracle Grid Infrastructure Installation Guide for your operating system for information about installing and configuring Oracle Grid Infrastructure

Example

The following example configures Oracle ASM Filter Driver on the node on which the command was run. `$ORACLE_HOME` in the example refers to the Oracle Grid Infrastructure home.

Example 29 Using the `afd_configure` command

```
# $ORACLE_HOME/bin/asmcmd afd_configure
```

afd_deconfigure**Purpose**

Deconfigures Oracle ASM Filter Driver.

Syntax and Description

```
# asmcmd afd_deconfigure
```

The `afd_deconfigure` command must be run noninteractively as a `root` user. Before running the command on a node, the Oracle Clusterware stack must be shut down on that node. After the `afd_deconfigure` command has been run, restart Oracle Clusterware on each node.

For information about Oracle ASM Filter Driver, refer to “[Oracle ASM Filter Driver](#)”.

See Also:

Oracle Grid Infrastructure Installation Guide for your operating system for information about installing and configuring Oracle Grid Infrastructure

Example

The following example deconfigures Oracle ASM Filter Driver on the node on which the command was run. `$ORACLE_HOME` in the example refers to the Oracle Grid Infrastructure home.

Example 30 Using the `afd_deconfigure` command

```
# $ORACLE_HOME/bin/asmcmd afd_deconfigure
```

afd_dsget**Purpose**

Retrieves the Oracle ASM Filter Driver discovery diskstring value.

Syntax and Description

```
afd_dsget
```

For information about Oracle ASM Filter Driver, refer to “[Oracle ASM Filter Driver](#)”.

Example

The following example returns the current Oracle ASM Filter Driver discovery diskstring value.

Example 31 Using the `afd_dsget` command

```
ASMCMD [+] > afd_dsget
AFD discovery string: /dev/rdsd/mydisks/*
```

afd_dsset

Purpose

Sets the Oracle ASM Filter Driver discovery diskstring value.

Syntax and Description

```
afd_dsset afd_diskstring
```

The syntax options for the `afd_dsset` command are described in [Table 24](#).

Table 24 Options for the `afd_dsset` command

Option	Description
<code>afd_diskstring</code>	Specifies the value for the Oracle ASM Filter Driver discovery diskstring.

For information about Oracle ASM Filter Driver, refer to “[Oracle ASM Filter Driver](#)”.

Example

The following example sets the current Oracle ASM Filter Driver discovery diskstring value.

Example 32 Using the `afd_dsset` command

```
ASMCMD [+] > afd_dsset /dev/rdsd/mydisks/*
```

afd_filter

Purpose

Sets the Oracle ASM Filter Driver filtering mode on a given disk path.

Syntax and Description

```
afd_filter {-e | -d } [disk_path]
```

The syntax options for the `afd_filter` command are described in the following table.

Table 25 Options for the `afd_filter` command

Option	Description
<code>-e</code>	Enables Oracle ASM Filter Driver mode.
<code>-d</code>	Disables Oracle ASM Filter Driver mode.
<code>disk_path</code>	Specifies the path to the disks.

If the command is executed without specifying a disk path, then filtering is set at the node level.

Example

The following example uses `afd_filter` to enable Oracle ASM Filter Driver filtering on a specified disk path.

Example 33 Using the `afd_filter` command

```
ASMCMD [+] > afd_filter -e /dev/sdq
```

afd_label

Purpose

Sets an Oracle ASM Filter Driver label to the specified disk.

Syntax and Description

```
afd_label afd_label disk_path [--migrate | --rename]
```

The syntax options for the `afd_label` command are described in [Table 26](#).

Table 26 Options for the `afd_label` command

Option	Description
<code>afd_label</code>	Specifies an Oracle ASM Filter Driver label.
<code>disk_path</code>	Specifies the path to the disks to which the label is applied.
<code>--migrate</code>	Specifies to migrate Oracle ASM Filter Driver disk labels to all disks in the <code>disk_path</code> .
<code>--rename</code>	Specifies to label a disk that was previously labeled.

For information about Oracle ASM Filter Driver, refer to [“Oracle ASM Filter Driver”](#).

Example

The following example sets an Oracle ASM Filter Driver label to a specified disk.

Example 34 Using the `afd_label` command

```
ASMCMD [+] > afd_label 'disk0' '/dev/rdisk/mydisks/disk0'
```

afd_lsdsdsk

Purpose

Lists Oracle ASM Filter Driver disks.

Syntax and Description

```
afd_lsdsdsk
```

Example

The following example lists Oracle ASM Filter Driver disks.

Example 35 Using the `afd_lsdsdsk` command

```
ASMCMD [+] > afd_lsdsdsk
```

```
-----
Label                Filtering    Path
-----
DISK0                ENABLED     /dev/sdd
DISK1                DISABLED   /dev/sdm
DISK2                ENABLED     /dev/sdq
-----
```

afd_scan

Purpose

Scans for Oracle ASM Filter Driver disks.

Syntax and Description

```
afd_scan [afd_diskstring]
```

The syntax options for the `afd_scan` command are described in [Table 27](#).

Table 27 Options for the `afd_scan` command

Option	Description
<code>afd_diskstring</code>	Specifies the value for the Oracle ASM Filter Driver discovery diskstring.

`afd_scan` scans for Oracle ASM Filter Driver disks using the specified discovery string. If the command is executed without specifying a disk string, then `afd_scan` uses the Oracle ASM Filter Driver discovery diskstring value in the `afd.conf` file.

For information about Oracle ASM Filter Driver, refer to “[Oracle ASM Filter Driver](#)”.

Example

The following example scans for Oracle ASM Filter Driver disks with a specified diskstring.

Example 36 Using the `afd_scan` command

```
ASMCMD [+] > afd_scan /dev/sd*
```

afd_state

Purpose

Returns the state of Oracle ASM Filter Driver.

Syntax and Description

```
afd_state
```

For information about Oracle ASM Filter Driver, refer to “[Oracle ASM Filter Driver](#)”.

Example

The following example returns the current state of Oracle ASM Filter Driver.

Example 37 Using the `afd_state` command

```
ASMCMD [+] > afd_state
ASMCMD-9526: The AFD state is 'LOADED' and filtering is 'DEFAULT' on host
'myhost'
```

afd_unlabel

Purpose

Clears a specified Oracle ASM Filter Driver label.

Syntax and Description

```
afd_unlabel afd_label
```

The syntax options for the `afd_unlabel` command are described in [Table 28](#).

Table 28 Options for the `afd_unlabel` command

Option	Description
<code>afd_unlabel</code>	Specifies an existing Oracle ASM Filter Driver label to clear.

For information about Oracle ASM Filter Driver, refer to [“Oracle ASM Filter Driver”](#).

Example

The following example clears an existing Oracle ASM Filter Driver label.

Example 38 Using the `afd_unlabel` command

```
ASMCMD [+] > afd_unlabel 'disk0'
```

ASMCMD File Management Commands

This section describes the ASMCMD file management commands.

[page 10-33](#) provides a summary of the file management commands.

Command	Description
amdu_extract	Extracts a file from a disk group.
cd	Changes the current directory to the specified directory.
cp	Enables you to copy files between disk groups, and between a disk group and the operating system.
du	Displays the total disk space occupied by files in the specified Oracle ASM directory and all of its subdirectories, recursively.
find	Lists the paths of all occurrences of the specified name (with wildcards) under the specified directory.
ls	Lists the contents of an Oracle ASM directory, the attributes of the specified file, or the names and attributes of all disk groups.
lsof	Lists the open files.
mkalias	Creates an alias for system-generated file names.
mkdir	Creates Oracle ASM directories.
pwd	Displays the path of the current Oracle ASM directory.
rm	Deletes the specified Oracle ASM files or directories.

Command	Description
ralias	Deletes the specified alias, retaining the file that the alias points to.

amdu_extract

Purpose

Extracts a file from a disk group.

Syntax and Description

```
amdu_extract diskgroup file_name disk_string
```

Table 30 Options for the amdu_extract command

Option	Description
<i>diskgroup</i>	Name of the disk group where the file is located.
<i>file_name</i>	Name of the file to extract. The file name must be an Oracle ASM alias name. The file name can be specified as an absolute or a relative path.
<i>disk_string</i>	Value for the Oracle ASM discovery diskstring.

`amdu_extract` calls the Oracle ASM Metadata Dump Utility (AMDU) command to extract a file using an Oracle ASM alias name.

Example

The following is an example of the `amdu_extract` command used to extract a file from the data disk group.

Example 39 Using the ASMCMD amdu_extract command

```
ASMCMD> amdu_extract data data/orcl/my_alias_filename /devices/disk*
```

cd

Purpose

Changes the current directory to the specified directory.

Syntax and Description

```
cd [dir]
```

[Table 31](#) lists the options for the `cd` command.

Table 31 Options for the cd command

Option	Description
<i>dir</i>	Name of the directory.

dir can be specified as either an absolute path or a relative path, including the `.` and `..` pseudo-directories. *dir* can contain wildcard characters. See [“Wildcard Characters”](#).

Examples

The following are examples of the `cd` command changing into various directories.

Example 40 Using the ASMCMD `cd` command

```
ASMCMD [+data/hr] > cd +data/orcl
ASMCMD [+data/orcl] > cd DATAFILE
ASMCMD [+data/orcl/DATAFILE] >cd ..
```

cp

Purpose

Enables you to copy files between Oracle ASM disk groups and between a disk group and the operating system.

Syntax and Description

```
cp src_file [--service service_name] [--port port_num] [connect_str:]tgt_file
```

Table 32 lists the syntax options for the `cp` command.

Table 32 Options for the `cp` command

Option	Description
<code>--service</code> <i>service_name</i>	Specifies the Oracle ASM instance name if not the default +ASM.
<code>--port</code> <i>port_num</i>	Specifies the listener port number. The default is 1521.
<i>connect_str</i>	Specifies the connection string for a remote instance.
<i>src_file</i>	Name of the source file to copy.
<i>tgt_file</i>	A user alias for the created target file name or an alias directory name.

`cp` cannot copy files between two remote instances. The local Oracle ASM instance must be either the source or the target of the operation.

You can use the `cp` command to:

- Copy files from a disk group to the operating system
- Copy files from a disk group to a disk group
- Copy files from the operating system to a disk group

Some file types cannot be the source or destination of the `cp` command. These file types include OCR and OCR backup file types. To back up, copy, or move an Oracle ASM SPFILE, use the `spbackup`, `spcopy`, or `spmmove` commands.

The format of copied files is portable between Little-Endian and Big-Endian systems if the files exist in an Oracle ASM disk group. Oracle ASM automatically converts the format when the files are written. For copying a non-Oracle ASM file from or to an Oracle ASM disk group, you can copy the file to a different endian platform and then use one of the commonly used utilities to convert the file.

connect_str is not required for a local instance copy, which is the default case. For a remote instance copy, you must specify the connect string and Oracle ASM prompts for a password in a non-echoing prompt. The *connect_str* is in the form:

```
user@host.SID
```

user, *host*, and *SID* are required in the *connect_str* parameter. The default port number is 1521 and can be changed with the `--port` option.

The connection privilege (SYSASM or SYSDBA) is determined by the use of the `--privilege` option when starting ASMCMD. For more information, refer to [“Specifying the Type of Connection”](#).

See Also:

Oracle Database Net Services Administrator’s Guide for more information about connection strings

src_file must be either a fully qualified file name or an Oracle ASM alias.

During an ASMCMD copy process, the Oracle ASM server creates an Oracle Managed File (OMF) file in the following format:

```
diskgroup/db_unique_name/file_type/file_name.##
```

where *db_uniq_name* is set to ASM and # is a string of digits. In the copy process, ASMCMD `cp` creates the directory structure for the destination and creates a user alias from that location to the actual OMF file that is created.

Examples

The following are examples of the `cp` command. The first example shows a copy of a file in the data disk group to a file on the operating system. The second example shows a copy of a file on the operating system to the data disk group. The third example shows how to copy a file in the data disk group to a remote server. You are prompted to enter a password.

Example 41 Using the ASMCMD cp command

```
ASMCMD [+] > cp +data/orcl/datafile/EXAMPLE.265.691577295 /mybackups/example.bak
copying +data/orcl/datafile/EXAMPLE.265.691577295 -> /mybackups/example.bak
```

```
ASMCMD [+] > cp /mybackups/examples.bak +data/orcl/datafile/myexamples.bak
copying /mybackups/examples.bak -> +data/orcl/datafile/myexamples.bak
```

```
ASMCMD [+] > cp +data/orcl/datafile/EXAMPLE.265.691577295 sys@myserver.+ASM:/
scratch/backup/myexamples.bak
Enter Password:
```

du

Purpose

Displays the total space used for files in the specified directory and in the entire directory tree under the directory.

Syntax and Description

```
du [--suppressheader] [dir]
```

Table 33 lists the syntax options for the `du` command.

Table 33 Options for the `du` command

Option	Description
<i>dir</i>	Name of the directory.
<code>--suppressheader</code>	Suppresses column headings from the output.

If you do not specify *dir*, then information about the current directory is displayed. *dir* can contain wildcard characters. See “[Wildcard Characters](#)”.

The following two values are displayed, both in units of megabytes.

- `Used_MB` - This value does not include mirroring.
- `Mirror_used_MB` - This value includes mirroring.

For example, if a normal redundancy disk group contains 100 MB of data and each file in the disk group is 2-way mirrored, then `Used_MB` is 100 MB and `Mirror_used_MB` is roughly 200 MB.

Example

The following is an example of the `du` command. The example shows disk space used in the `orcl` directory in the `data` disk group, including all of the directories under the `orcl` directory.

Example 42 Using the ASMCMD `du` command

```
ASMCMD [+] > du data/orcl
Used_MB      Mirror_used_MB
  1756                3519
```

find

Purpose

Displays the absolute paths of all occurrences of the specified name pattern (with wildcards) in a specified directory and its subdirectories.

Syntax and Description

```
find [--type type] dir pattern
```

Table 34 lists the syntax options for the `find` command.

Table 34 Options for the `find` command

Option	Description
<code>--type type</code>	Type of target to find.
<i>dir</i>	Directory name where you want to start searching.
<i>pattern</i>	Name of a target or a wildcard pattern.

This command searches the specified directory and all subdirectories under it in the directory tree for the supplied *pattern*. The value used for *pattern* can be a directory name or a file name, and can include wildcard characters. See “[Wildcard Characters](#)”.

The ASMCMD `find` command is case insensitive.

In the output of the command, directory names are suffixed with the slash character (/) to distinguish them from file names.

Use the `--type` flag to find all the files of a particular type (specified as *type*). For example, you can search for control files by specifying *type* as `CONTROLFILE`. Valid values for *type* are listed in [Table 1](#). These are type values from the *type* column of the `V$ASM_FILE` view.

Examples

The following are examples of the `find` command. The first example searches the data disk group for files that begin with `undo`. The second example returns the absolute path of all the control files (`--type CONTROLFILE`) in the `+data/orcl` directory.

Example 43 Using the ASMCMD find command

```
ASMCMD [+] > find +data undo*
+data/ORCL/DATAFILE/UNDOTBS1.258.691577151

ASMCMD [+] > find --type CONTROLFILE +data/orcl *
+data/orcl/CONTROLFILE/Current.260.691577263
```

ls

Purpose

Lists the contents of an Oracle ASM directory, the attributes of the specified file, or the names and attributes of all disk groups.

Syntax and Description

```
ls [--suppressheader] [-lsdtLg][--absolutepath][--reverse]
  [--permission][pattern]
```

[Table 35](#) lists the syntax options for the `ls` command.

Table 35 Options for the ls command

Option	Description
(none)	Displays only file names and directory names.
-l	Displays extended file information, including striping and redundancy information and whether the file was system-generated (indicated by Y under the <code>SYS</code> column) or user-created (as with an alias, indicated by N under the <code>SYS</code> column). When used in the " <code>ls -l +</code> " command, displays directory information. Not all possible file attributes or disk group attributes are included. To view the complete set of column values for a file or a disk group, query the <code>V\$ASM_FILE</code> and <code>V\$ASM_DISKGROUP</code> views.
-s	Displays file space information.
-d	If the value for the <i>pattern</i> argument is a directory, then <code>ls</code> displays information about that directory, rather than the directory contents. Typically used with another flag, such as the <code>-l</code> flag.
--reverse	Reverses the sort order of the listing.
-t	Sorts the listing by timestamp (latest first) instead of by name.

Option	Description
-L	If the value for the <i>pattern</i> argument is an alias, then ASMCMD displays information about the file that it references. Typically used with another flag, such as the -l flag.
--absolutepath	For each listed file, displays the absolute path of the alias that references it, if any.
-g	GV\$ASM_DISKGROUP.INST_ID is included in the output.
--suppressheader	Suppresses column headings.
--permission	Shows the permissions of a file (V\$ASM_FILE.permission, V\$ASM_FILE.owner, V\$ASM_FILE.usergroup, V\$ASM_ALIAS.name).
<i>pattern</i>	Name of a file, directory, or a pattern.

Command options enable you to modify and customize the output of the command. [Table 35](#) lists the options and their descriptions. For disk group information, this command queries the V\$ASM_DISKGROUP_STAT view by default. If you specify all of the options, then the command shows a union of their attributes, with duplicates removed. If you enter `ls +`, the top level directory structure is displayed.

pattern can be a file name, directory name, or a pattern including wildcard characters. See [“Wildcard Characters”](#).

- If *pattern* is a directory name, then `ls` lists the contents of the directory and depending on flag settings, `ls` also lists information about each directory member. Directories are listed with a trailing slash (/) to distinguish them from files.
- If the value that you enter for *pattern* is a file name, then `ls` lists the file and depending on the flag settings, `ls` also lists information about the file. The file must be located in the current directory if the file name is specified with a relative path.

Examples

The following are examples of the `ls` command that display various information about directories and the contents of the directories.

Example 44 Using the ASMCMD ls command

```
ASMCMD [+] > ls +data/orcl/datafile
EXAMPLE.265.691577295
SYS_AUX.257.691577149
SYSTEM.256.691577149
UNDOTBS1.258.691577151
USERS.259.691577151
```

```
ASMCMD [+] > ls -lt +data/orcl/datafile
Type      Redund  Striped  Time                Sys  Name
DATAFILE  MIRROR  COARSE   JUL 13 08:00:00    Y    EXAMPLE.265.691577295
DATAFILE  MIRROR  COARSE   JUL 13 05:00:00    Y    SYS_AUX.257.691577149
DATAFILE  MIRROR  COARSE   JUL 13 02:00:00    Y    USERS.259.691577151
DATAFILE  MIRROR  COARSE   JUL 13 02:00:00    Y    UNDOTBS1.258.691577151
DATAFILE  MIRROR  COARSE   JUL 13 02:00:00    Y    SYSTEM.256.691577149
```

```
ASMCMD [+] > ls -l +data/orcl/datafile/sy*
Type      Redund  Striped  Time                Sys  Name
DATAFILE  MIRROR  COARSE   JUL 13 05:00:00    Y    SYS_AUX.257.691577149
DATAFILE  MIRROR  COARSE   JUL 13 02:00:00    Y    SYSTEM.256.691577149
```

```

ASMCMD [+] > ls -s +data/orcl/datafile
Block_Size  Blocks      Bytes      Space  Name
      8192   12801   104865792   214958080  EXAMPLE.265.691577295
      8192   88321   723525632   1452277760  SYSAUX.257.691577149
      8192   88321   723525632   1452277760  SYSTEM.256.691577149
      8192    7681   62922752    131072000  UNDOTBS1.258.691577151
      8192     641    5251072     12582912  USERS.259.691577151

ASMCMD [+] > ls --permission +data/orcl/datafile
User  Group  Permission  Name
      rw-rw-rw-  EXAMPLE.265.691577295
      rw-rw-rw-  SYSAUX.257.691577149
      rw-rw-rw-  SYSTEM.256.691577149
      rw-rw-rw-  UNDOTBS1.258.691577151
      rw-rw-rw-  USERS.259.691577151
    
```

Isof

Purpose

Lists the open files of the local clients.

Syntax and Description

```
lsof [--suppressheader] [-G diskgroup | --dbname db | -C instance]
```

[Table 36](#) lists the syntax options for the `lsof` command.

Table 36 Options for the `lsof` command

Option	Description
<code>--suppressheader</code>	Suppresses column headings.
<code>-G <i>diskgroup</i></code>	List files only from the specified disk group.
<code>--dbname <i>db</i></code>	List files only from the specified database.
<code>-C <i>instance</i></code>	List files only from the specified instance.

Example

The following are examples of the `lsof` command. The first example lists the open files for the data disk group. The second example lists the open files for the Oracle ASM instance.

Example 45 Using the ASMCMD `lsof` command

```

ASMCMD [+] > lsof -G data
DB_Name  Instance_Name  Path
orcl     orcl           +data/orcl/controlfile/current.260.691577263
orcl     orcl           +data/orcl/datafile/example.265.691577295
orcl     orcl           +data/orcl/datafile/sysaux.257.691577149
orcl     orcl           +data/orcl/datafile/system.256.691577149
orcl     orcl           +data/orcl/datafile/undotbs1.258.691577151
orcl     orcl           +data/orcl/datafile/users.259.691577151
orcl     orcl           +data/orcl/onlinelog/group_1.261.691577267
orcl     orcl           +data/orcl/onlinelog/group_2.262.691577271
orcl     orcl           +data/orcl/onlinelog/group_3.263.691577275
orcl     orcl           +data/orcl/tempfile/temp.264.691577287

ASMCMD [+] > lsof -C +ASM
DB_Name  Instance_Name  Path
asmvol   +ASM           +data/VOLUME1.271.679226013
asmvol   +ASM           +data/VOLUME2.272.679227351
    
```

mkalias

Purpose

Creates an alias for the specified system-generated file name.

Syntax and Description

```
mkalias file alias
```

[Table 37](#) lists the syntax options for the `mkalias` command.

Table 37 Options for the `mkalias` command

Option	Description
<i>file</i>	System-generated file name.
<i>alias</i>	Alias for the file name.

alias must be in the same disk group as the system-generated file. Only one alias is permitted for each Oracle ASM file.

Example

The following example creates the `sysaux.f` alias for the fully qualified file name `+data/orcl/DATAFILE/SYSAUX.257.721811945`. Following the `mkalias` command, `ls --absolutepath` is run to check the results.

Example 46 Using the ASMCMD `mkalias` command

```
ASMCMD [+data/orcl/datafile] > mkalias SYSAUX.257.721811945 sysaux.f

ASMCMD [+data/orcl/datafile] > ls --absolutepath
none => EXAMPLE.265.721812093
+DATA/ORCL/DATAFILE/sysaux.f => SYSAUX.257.721811945
none => SYSTEM.256.721811945
none => UNDOTBS1.258.721811945
none => USERS.259.721811947
sysaux.f
```

mkdir

Purpose

Creates Oracle ASM directories under the current directory.

Syntax and Description

```
mkdir dir [dir . . .]
```

[Table 38](#) lists the syntax options for the `mkdir` command.

Table 38 Options for the `mkdir` command

Option	Description
<i>dir</i>	Directory name to create.

The directory from which `mkdir` is run can be a system-created or user-created directory. You cannot create a directory at the root (+) level.

Example

The following is an example of the `mkdir` command. The example creates the directories `subdir1` and `subdir2` at the disk group level in the disk group `data`.

Example 47 Using the ASMCMD mkdir command

```
ASMCMD [+data] > mkdir subdir1 subdir2

ASMCMD [+data] > ls
ASM/
ORCL/
subdir1/
subdir2/
```

pwd

Purpose

Displays the absolute path of the current directory.

Syntax and Description

```
pwd
```

Example

The following is an example of the `pwd` command. The example displays the current directory.

Example 48 Using the ASMCMD pwd command

```
ASMCMD [+data/orcl/datafile] > pwd
+data/orcl/datafile
```

rm

Purpose

Deletes the specified Oracle ASM files and directories.

Syntax and Description

```
rm [-f|-r] pattern [pattern...]
```

[Table 39](#) lists the syntax options for the `rm` command.

Table 39 Options for the rm command

Option	Description
<code>-r</code>	Recursively deletes files and subdirectories.
<code>-f</code>	Deletes files and subdirectories without prompting for confirmation.
<code>pattern</code>	Name of a file, directory, or wildcard pattern.

If `pattern` is a file or alias, then the `rm` command can delete the file or alias only if it is not currently in use. If `pattern` is a directory, then the `rm` command can delete it only if it is empty (unless the `-r` flag is used) and it is not a system-generated directory. If `pattern` is an alias, then the `rm` command deletes both the alias and the

file to which the alias refers. To delete only an alias and retain the file that the alias references, use the `rmalias` command.

Note:

When you delete all of the files in a system-created directory, the directory is removed. If the parent directories are empty, all of the parent directories are also removed.

pattern can contain wildcard characters. See “[Wildcard Characters](#)”.

If you use a wildcard, the `rm` command deletes all of the matches except nonempty directories, unless you use the `-r` flag. To recursively delete, use the `-r` flag. With `-r` option you can delete a nonempty directory, including all files and directories in it and in the entire directory tree underneath it. If you use the `-r` flag or a wildcard character, then the `rm` command prompts you to confirm the deletion before proceeding, unless you specify the `-f` flag. If a wildcard character matches an alias or a system-generated file that has an alias, then both the alias and the system-generated file that it references are deleted. When using the `-r` flag to delete an alias that matches a wildcard pattern, either the alias or the system-generated file that has an alias must be present in the directory in which you run the `rm` command.

For example, if you have a user alias, `+data/dir1/file.alias` that points to `+data/orcl/DATAFILE/System.256.146589651`, then running the `rm -r +data/dir1` command removes the `+data/dir1/file.alias` and `+data/orcl/DATAFILE/System.256.146589651`.

Example

The following are examples of the `rm` command. The first example deletes the `myexamples.bak` file. The second example removes the `subdir2` directory and its contents.

Example 49 Using the ASMCMD rm command

```
ASMCMD [+data/orcl/datafile] > rm myexamples.bak

ASMCMD [+data] > rm -r subdir2
You may delete multiple files and/or directories.
Are you sure? (y/n) y
```

rmalias

Purpose

Removes the specified aliases, retaining the files that the aliases reference.

Syntax and Description

```
rmalias [-r] alias [alias...]
```

[Table 40](#) lists the syntax options for the `rmalias` command.

Table 40 Options for the *rmalias* command

Option	Description
<code>-r</code>	Recursively removes aliases.

Option	Description
<i>alias</i>	Alias for the file name or directory.

The `-r` flag enables you to remove all of the aliases in the current directory and in the entire directory tree beneath the current directory. If any user-created directories become empty after deleting aliases, they are also deleted. Files and directories created by the system are not deleted.

Example

The following is an example of the `rmalias` command. The example deletes the alias `sysaux.f`, retaining the data file that it references.

Example 50 Using the ASMCMD `rmalias` command

```
ASMCMD [+data/orcl/datafile] > rmalias sysaux.f
```

ASMCMD Disk Group Management Commands

This section describes the ASMCMD disk group management commands.

[page 10-44](#) provides a summary of the disk group management commands.

Command	Description
chdg	Changes a disk group (add, drop, or rebalance).
chkdg	Checks or repairs a disk group.
dropdg	Drops a disk group.
iostat	Displays I/O statistics for disks.
lsattr	Lists the attributes of a disk group.
lsdg	Lists disk groups and their information.
lsdsk	Lists disks Oracle ASM disks.
lsod	Lists open devices.
md_backup	Creates a backup of the metadata of mounted disk groups.
md_restore	Restores disk groups from a backup of the metadata.
mkdg	Creates a disk group.
mount	Mounts a disk group.
offline	Offlines a disk or a failure group.
online	Onlines a disk or a failure group.
rebal	Rebalances a disk group.
remap	Relocates data in a range of physical blocks on a disk.
setattr	Sets attributes in a disk group.
umount	Dismounts a disk group.

chdg

Purpose

Changes a disk group (adds disks, drops disks, resizes disks, or rebalances a disk group) based on an XML configuration file.

Syntax and Description

```
chdg { config_file.xml | 'contents_of_xml_file' }
```

Table 42 lists the syntax options for the chdg command.

Table 42 Options for the chdg command

Option	Description
<i>config_file</i>	Name of the XML file that contains the changes for the disk group. chdg searches for the XML file in the directory where ASMCMD was started unless a path is specified. For examples of the valid tags and XML configuration file, see Example 51 and Example 52 .
<i>contents_of_xml_file</i>	The XML script enclosed in single quotations.

chdg modifies a disk group based on an XML configuration file. The modification includes adding, replacing, or deleting disks from an existing disk group, and the setting rebalance or replace power level. The power level can be set to the same values as the ASM_POWER_LIMIT initialization parameter. For information about the initialization parameter, see “[ASM_POWER_LIMIT](#)”.

When adding disks to a disk group, the diskstring must be specified in a format similar to the ASM_DISKSTRING initialization parameter. For information about the initialization parameter, see “[ASM_DISKSTRING](#)”.

The failure groups are optional parameters. The default causes every disk to belong to a its own failure group. For information about failure groups, see “[Oracle ASM Failure Groups](#)”.

Dropping disks from a disk group can be performed through this operation. An individual disk can be referenced by its Oracle ASM disk name. A set of disks that belong to a failure group can be specified by the failure group name. For information about dropping disks, see “[Dropping Disks from Disk Groups](#)”.

You can resize a disk inside a disk group with chdg. The resize operation fails if there is not enough space for storing data after the resize. For information about resizing disks, see “[Resizing Disks in Disk Groups](#)”.

[Example 51](#) shows the basic structure and the valid tags with their respective attributes for the chdg XML configuration file.

Example 51 Tags for the chdg XML configuration template

```
<chdg> update disk clause (add/delete disks/failure groups)
      name          disk group to change
      power         power to perform rebalance or replace

<add>  items to add are placed here
</add>

<replace> items to replace are placed here
</replace>
```

```

<drop> items to drop are placed here
</drop>

<fg> failure group
      name          failure group name
</fg>

<dsk> disk
      name          disk name
      string        disk path
      size          size of the disk to add
      force         true specifies to use the force option
</dsk>

</chdg>
    
```

For information about creating a disk group with ASMCMD `mkdgm`, see “[mkdgm](#)”. For information about altering disk groups, see “[Altering Disk Groups](#)”.

Example

The following is an example of an XML configuration file for `chdg`. This XML file alters the disk group named `data`. The failure group `fg1` is dropped and the disk `data_0001` is also dropped. The `/dev/disk5` disk is added to failure group `fg2`. The rebalance power level is set to 3.

Example 52 *chdg sample XML configuration file*

```

<chdg name="data" power="3">
  <drop>
    <fg name="fg1"></fg>
    <dsk name="data_0001"/>
  </drop>
  <add>
    <fg name="fg2">
      <dsk string="/dev/disk5"/>
    </fg>
  </add>
</chdg>
    
```

The following are examples of the `chdg` command with the configuration file or configuration information on the command line.

Example 53 *Using the ASMCMD chdg command*

```

ASMCMD [+] > chdg data_config.xml

ASMCMD [+] > chdg '<chdg name="data" power="3">
  <drop><fg name="fg1"></fg><dsk name="data_0001"/></drop>
  <add><fg name="fg2"><dsk string="/dev/disk5"/></fg></add></chdg>'
    
```

chkdgm

Purpose

Checks or repairs the metadata of a disk group.

Syntax and Description

```
chkdgm [--repair] diskgroup
```

[Table 43](#) lists the syntax options for the `chkdgm` command.

Table 43 Options for the *chkdg* command

Option	Description
<code>--repair</code>	Repairs the disk group.
<i>diskgroup</i>	Name of disk group to check or repair.

chkdg checks the metadata of a disk group for errors and optionally repairs the errors.

Example

The following is an example of the *chkdg* command used to check and repair the data disk group.

Example 54 Using the ASMCMD *chkdg* command

```
ASMCMD [+] > chkdg --repair data
```

dropdg

Purpose

Drops a disk group.

Syntax and Description

```
dropdg [-r [-f]] diskgroup
```

[Table 44](#) lists the syntax options for the *dropdg* command.

Table 44 Options for the *dropdg* command

Option	Description
<code>-f</code>	Force the operation. Only applicable if the disk group cannot be mounted.
<code>-r</code>	Recursive, include contents.
<i>diskgroup</i>	Name of disk group to drop.

dropdg drops an existing disk group. The disk group should not be mounted on multiple nodes.

Example

These are examples of the use of *dropdg*. The first example forces the drop of the disk group *data*, including any data in the disk group. The second example drops the disk group *fra*, including any data in the disk group.

Example 55 Using the ASMCMD *dropdg* command

```
ASMCMD [+] > dropdg -r -f data
```

```
ASMCMD [+] > dropdg -r fra
```

iostat

Purpose

Displays I/O statistics for Oracle ASM disks in mounted disk groups.

Syntax and Description

```
iostat [--suppressheader] [-et] [--io] [--region]
      [-G diskgroup] [interval]
```

`iostat` lists disk group statistics using the `V$ASM_DISK_IOSTAT` view.

[Table 45](#) lists the syntax options for the `iostat` command.

Table 45 Options for the `iostat` command

Option	Description
<code>-e</code>	Displays error statistics (Read_Err, Write_Err).
<code>-G <i>diskgroup</i></code>	Displays statistics for the disk group name.
<code>--suppressheader</code>	Suppresses column headings.
<code>--io</code>	Displays information in number of I/Os, instead of bytes.
<code>-t</code>	Displays time statistics (Read_Time, Write_Time).
<code>--region</code>	Displays information for cold and hot disk regions (Cold_Reads, Cold_Writes, Hot_Reads, Hot_Writes).
<i>interval</i>	Refreshes the statistics display based on the interval value (seconds). Use CTRL+C to stop the interval display.

[Table 46](#) shows the statistics for a disk group. To view the complete set of statistics for a disk group, use the `V$ASM_DISK_IOSTAT` view.

Table 46 Attribute descriptions for `iostat` command output

Attribute Name	Description
Group_Name	Name of the disk group.
Dsk_Name	Name of the disk.
Reads	Number of bytes read from the disk. If the <code>--io</code> option is entered, then the value is displayed as number of I/Os.
Writes	Number of bytes written to the disk. If the <code>--io</code> option is entered, then the value is displayed as number of I/Os.
Cold_Reads	Number of bytes read from the cold disk region. If the <code>--io</code> option is entered, then the value is displayed as number of I/Os.
Cold_Writes	Number of bytes written from the cold disk region. If the <code>--io</code> option is entered, then the value is displayed as number of I/Os.
Hot_Reads	Number of bytes read from the hot disk region. If the <code>--io</code> option is entered, then the value is displayed as number of I/Os.
Hot_Writes	Number of bytes written to the hot disk region. If the <code>--io</code> option is entered, then the value is displayed as number of I/Os.
Read_Err	Number of failed I/O read requests for the disk.
Write_Err	Number of failed I/O write requests for the disk.
Read_Time	I/O time (in seconds) for read requests for the disk if the <code>TIMED_STATISTICS</code> initialization parameter is set to <code>TRUE</code> (0 if set to <code>FALSE</code>).
Write_Time	I/O time (in seconds) for write requests for the disk if the <code>TIMED_STATISTICS</code> initialization parameter is set to <code>TRUE</code> (0 if set to <code>FALSE</code>).

If a refresh interval is not specified, the number displayed represents the total number of bytes or I/Os. If a refresh interval is specified, then the value displayed (bytes or I/Os) is the difference between the previous and current values, not the total value.

Example

The following are examples of the `iostat` command. The first example displays disk I/O statistics for the data disk group in total number of bytes. The second example displays disk I/O statistics for the data disk group in total number of I/O operations.

Example 56 Using the ASMCMD iostat command

```
ASMCMD [+] > iostat -G data
Group_Name Dsk_Name Reads Writes
DATA DATA_0000 180488192 473707520
DATA DATA_0001 1089585152 469538816
DATA DATA_0002 191648256 489570304
DATA DATA_0003 175724032 424845824
DATA DATA_0004 183421952 781429248
DATA DATA_0005 1102540800 855269888
DATA DATA_0006 171290624 447662592
DATA DATA_0007 172281856 361337344
DATA DATA_0008 173225472 390840320
DATA DATA_0009 288497152 838680576
DATA DATA_0010 196657152 375764480
DATA DATA_0011 436420096 356003840
```

```
ASMCMD [+] > iostat --io -G data
Group_Name Dsk_Name Reads Writes
DATA DATA_0000 2801 34918
DATA DATA_0001 58301 35700
DATA DATA_0002 3320 36345
DATA DATA_0003 2816 10629
DATA DATA_0004 2883 34850
DATA DATA_0005 59306 38097
DATA DATA_0006 2151 10129
DATA DATA_0007 2686 10376
DATA DATA_0008 2105 8955
DATA DATA_0009 9121 36713
DATA DATA_0010 3557 8596
DATA DATA_0011 17458 9269
```

lsattr

Purpose

Lists the attributes of a disk group.

Syntax and Description

```
lsattr [--suppressheader][-G diskgroup ] [-lm] [pattern]
```

[Table 47](#) lists the syntax options for the `lsattr` command.

Table 47 Options for the lsattr command

Option	Description
<code>-G diskgroup</code>	Disk group name.
<code>--suppressheader</code>	Suppresses column headings.
<code>-l</code>	Display names with values.

Option	Description
-m	Displays additional information, such as the RO and Sys columns.
<i>pattern</i>	Display the attributes that contain pattern expression.

Information about disk group attributes is retrieved from the `V$ASM_ATTRIBUTE` view. For information about disk group attributes, see [“Managing Disk Group Attributes”](#).

The RO (read-only) column identifies those attributes that can only be set when a disk group is created. The Sys column identifies those attributes that are system-created.

To display information about the disk group template attributes, see [“lstmpl”](#).

To set disk group attributes, see [“setattr”](#).

Example

The following are examples of the `lsattr` command. The first displays information about all attributes for the `data` disk group. The second example displays only those attributes with names containing the string `compat` for the `fra` disk group. Note the use of both the `%` and `*` wildcard characters on Linux.

Example 57 Using the ASMCMD lsattr command

```
ASMCMD [+] > lsattr -lm -G data
Group_Name Name Value RO Sys
DATA access_control.enabled FALSE N Y
DATA access_control.umask 066 N Y
DATA au_size 1048576 Y Y
DATA cell.smart_scan_capable FALSE N N
DATA cell.sparse_dg allnonsparse N N
DATA compatible.advm 12.1.0.2.0 N Y
DATA compatible.asm 12.1.0.2.0 N Y
DATA compatible.rdbms 12.1.0.0.0 N Y
DATA content.check FALSE N Y
DATA content.type data N Y
DATA disk_repair_time 3.6h N Y
DATA failgroup_repair_time 24.0h N Y
DATA idp.boundary auto N Y
DATA idp.type dynamic N Y
DATA phys_meta_replicated true Y Y
DATA sector_size 512 Y Y
DATA thin_provisioned FALSE N Y
```

```
ASMCMD [+] > lsattr -G fra -l %compat*
Name Value
compatible.asm 12.1.0.0.0
compatible.rdbms 11.2.0.3.0
```

lsdg

Purpose

Lists mounted disk groups and their information. `lsdg` queries `V $ASM_DISKGROUP_STAT` by default. If the `--discovery` flag is specified, the `V $ASM_DISKGROUP` is queried instead. The output also includes notification of any current rebalance operation for a disk group. If a disk group is specified, then `lsdg` returns only information about that disk group.

Syntax and Description

```
lsdg [--suppressheader] [-g] [--discovery] [pattern]
```

Table 48 lists the options for the `lsdg` command.

Table 48 Options for the `lsdg` command

Option	Description
(none)	Displays the disk group attributes listed in Table 49 .
<code>--discovery</code>	Selects from <code>V\$ASM_DISKGROUP</code> , or from <code>GV\$ASM_DISKGROUP</code> if the <code>-g</code> flag is also specified. This option is always enabled if the Oracle ASM instance is version 10.1 or earlier. This flag is disregarded if <code>lsdg</code> is running in non-connected mode.
<code>-g</code>	Selects from <code>GV\$ASM_DISKGROUP_STAT</code> , or from <code>GV\$ASM_DISKGROUP</code> if the <code>--discovery</code> flag is also specified. <code>GV\$ASM_DISKGROUP.INST_ID</code> is included in the output. The <code>REBAL</code> column of the <code>GV\$ASM_OPERATION</code> view is also included in the output.
<code>--suppressheader</code>	Suppresses column headings.
<i>pattern</i>	Returns only information about the specified disk group or disk groups that match the supplied pattern. See “ Wildcard Characters ”.

Table 49 shows the attributes for each disk group. To view the complete set of attributes for a disk group, use the `V$ASM_DISKGROUP_STAT` or `V$ASM_DISKGROUP` view.

See Also:

Oracle Database Reference for descriptions of disk group information displayed in the `V$ASM_DISKGROUP` view

Table 49 Attribute descriptions for `lsdg` command output

Attribute Name	Description
State	State of the disk group. Values include <code>BROKEN</code> , <code>CONNECTED</code> , <code>DISMOUNTED</code> , <code>MOUNTED</code> , <code>QUIESCING</code> , and <code>UNKNOWN</code> .
Type	Disk group redundancy (<code>NORMAL</code> , <code>HIGH</code> , <code>EXTERNAL</code>).
Rebal	Y if a rebalance operation is in progress.
Sector	Sector size in bytes.
Block	Block size in bytes.
AU	Allocation unit size in bytes.
Total_MB	Size of the disk group in megabytes.
Free_MB	Free space in the disk group in megabytes, without regard to redundancy. From the <code>V\$ASM_DISKGROUP</code> view.
Req_mir_free_MB	Amount of space that must be available in the disk group to restore full redundancy after the most severe failure that can be tolerated by the disk group. This is the <code>REQUIRED_MIRROR_FREE_MB</code> column from the <code>V\$ASM_DISKGROUP</code> view.

Attribute Name	Description
Usable_file_MB	Amount of free space, adjusted for mirroring, that is available for new files. From the V\$ASM_DISKGROUP view.
Offline_disks	Number of offline disks in the disk group. Offline disks are eventually dropped.
Voting_files	Specifies whether the disk group contains voting files (Y or N).
Name	Disk group name.

Example

The following example lists the attributes of the data disk group.

Example 58 Using the ASMCMD lsdg command

```
ASMCMD [+] > lsdg data
State   Type   Rebal  Sector  Block      AU  Total_MB  Free_MB  Req_mir_free_MB
Usable_file_MB
MOUNTED NORMAL  N           512   4096  4194304    12288    8835           1117
3859

(continued)
Offline_disks  Voting_files  Name
              0              N  DATA
```

lsdsk

Purpose

Lists Oracle ASM disks.

Syntax and Description

```
lsdsk [--suppressheader] [-kptgMI] [-G diskgroup ]
      [ --member|--candidate]
      [--discovery][--statistics][pattern]
```

Table 50 lists the options for the lsdsk command.

Table 50 Options for the lsdsk command

Option	Description
(none)	Displays the PATH column of the V\$ASM_DISK_STAT view.
-k	Displays the TOTAL_MB, FREE_MB, OS_MB, NAME, FAILGROUP, LIBRARY, LABEL, UDID, PRODUCT, REDUNDANCY, and PATH columns of the V\$ASM_DISK view.
--statistics	Displays the READS, WRITES, READ_ERRS, WRITE_ERRS, READ_TIME, WRITE_TIME, BYTES_READ, BYTES_WRITTEN, and the PATH columns of the V\$ASM_DISK view.
-p	Displays the GROUP_NUMBER, DISK_NUMBER, INCARNATION, MOUNT_STATUS, HEADER_STATUS, MODE_STATUS, STATE, and the PATH columns of the V\$ASM_DISK view.
-t	Displays the CREATE_DATE, MOUNT_DATE, REPAIR_TIMER, and the PATH columns of the V\$ASM_DISK view.

Option	Description
-g	Selects from GV\$ASM_DISK_STAT, or from GV\$ASM_DISK if the --discovery flag is also specified. GV\$ASM_DISK.INST_ID is included in the output.
--discovery	Selects from V\$ASM_DISK, or from GV\$ASM_DISK if the -g flag is also specified. This option is always enabled if the Oracle ASM instance is version 10.1 or earlier. This flag is disregarded if lsdsk is running in non-connected mode.
--suppressheader	Suppresses column headings.
-I	Scans disk headers for information rather than extracting the information from an Oracle ASM instance. This option forces non-connected mode.
-G	Restricts results to only those disks that belong to the group specified by <i>diskgroup</i> .
-M	Displays the disks that are visible to some but not all active instances. These are disks that, if included in a disk group, cause the mount of that disk group to fail on the instances where the disks are not visible.
--candidate	Restricts results to only disks having membership status equal to CANDIDATE.
--member	Restricts results to only disks having membership status equal to MEMBER.
<i>pattern</i>	Returns only information about the specified disks that match the supplied pattern.

The `lsdsk` command can run in connected or non-connected mode. The connected mode is always attempted first. The `-I` option forces non-connected mode.

- In connected mode, `lsdsk` uses the `V$ASM_DISK_STAT` and `V$ASM_DISK` dynamic views to retrieve disk information. The `V$ASM_DISK_STAT` view is used by default.
- In non-connected mode, `lsdsk` scans disk headers to retrieve disk information. Some information is not available in this mode and some options are not valid combinations with this mode.

Note:

The non-connected mode is not supported on Windows.

pattern restricts the output to only disks that match the pattern specified. Wild-card characters and slashes (/ or \) can be part of the pattern. *pattern* should be specified as the last option for the command. For information about wildcards, see [“Wildcard Characters”](#).

The `-k`, `-p`, `-t`, and `--statistics` options modify how much information is displayed for each disk. If any combination of the options are specified, then the output shows the union of the attributes associated with each flag.

Example

The following are examples of the `lsdisk` command. The first and second examples list information about disks in the `data` disk group. The third example lists information about candidate disks.

Example 59 Using the ASMCMD `lsdisk` command

```
ASMCMD [+] > lsdisk -t -G data
Create_Date  Mount_Date  Repair_Timer  Path
13-JUL-09    13-JUL-09    0              /devices/diska1
13-JUL-09    13-JUL-09    0              /devices/diska2
13-JUL-09    13-JUL-09    0              /devices/diska3
13-JUL-09    13-JUL-09    0              /devices/diskb1
13-JUL-09    13-JUL-09    0              /devices/diskb2
13-JUL-09    13-JUL-09    0              /devices/diskb3
13-JUL-09    13-JUL-09    0              /devices/diskc1
13-JUL-09    13-JUL-09    0              /devices/diskc2
...

ASMCMD [+] > lsdisk -p -G data /devices/diska*
Group_Num  Disk_Num      Incarn  Mount_Stat  Header_Stat  Mode_Stat  State  Path
1          0      2105454210  CACHED     MEMBER       ONLINE    NORMAL /devices/diska1
1          1      2105454199  CACHED     MEMBER       ONLINE    NORMAL /devices/diska2
1          2      2105454205  CACHED     MEMBER       ONLINE    NORMAL /devices/diska3

ASMCMD [+] > lsdisk --candidate -p
Group_Num  Disk_Num      Incarn  Mount_Stat  Header_Stat  Mode_Stat  State  Path
0          5      2105454171  CLOSED    CANDIDATE    ONLINE    NORMAL /devices/diske1
0          25     2105454191  CLOSED    CANDIDATE    ONLINE    NORMAL /devices/diske2
0          18     2105454184  CLOSED    CANDIDATE    ONLINE    NORMAL /devices/diske3
0          31     2105454197  CLOSED    CANDIDATE    ONLINE    NORMAL /devices/diskk1
0          21     2105454187  CLOSED    CANDIDATE    ONLINE    NORMAL /devices/diskk2
0          26     2105454192  CLOSED    CANDIDATE    ONLINE    NORMAL /devices/diskk3
0          14     2105454180  CLOSED    CANDIDATE    ONLINE    NORMAL /devices/diskl1
...
```

lsod

Purpose

Lists the open Oracle ASM disks.

Syntax and Description

```
lsod [--suppressheader] [-G diskgroup] [--process process] [pattern]
```

[Table 51](#) lists the syntax options for the `lsod` command.

Table 51 Options for the `lsod` command

Option	Description
<code>--suppressheader</code>	Suppresses column header information from the output.
<code>-G <i>diskgroup</i></code>	Specifies the disk group that contains the open disks.
<code>--process <i>process</i></code>	Specifies a pattern to filter the list of processes.
<i>pattern</i>	Specifies a pattern to filter the list of disks.

The rebalance operation (RBAL) opens a disk both globally and locally so the same disk may be listed twice in the output for the RBAL process.

Example

The following are examples of the `lsod` command. The first example lists the open devices associated with the data disk group and the LGWR process. The second example lists the open devices associated with the LGWR process for disks that match the `diska` pattern.

Example 60 Using the ASMCMD `lsod` command

```
ASMCMD [+] > lsod -G data --process *LGWR*
Instance Process                OSPID Path
1         oracle@myserver02 (LGWR) 26593 /devices/diska1
1         oracle@myserver02 (LGWR) 26593 /devices/diska2
1         oracle@myserver02 (LGWR) 26593 /devices/diska3
1         oracle@myserver02 (LGWR) 26593 /devices/diskb1
1         oracle@myserver02 (LGWR) 26593 /devices/diskb2
1         oracle@myserver02 (LGWR) 26593 /devices/diskb3
1         oracle@myserver02 (LGWR) 26593 /devices/diskd1

ASMCMD [+] > lsod --process *LGWR* *diska*
Instance Process                OSPID Path
1         oracle@myserver02 (LGWR) 26593 /devices/diska1
1         oracle@myserver02 (LGWR) 26593 /devices/diska2
1         oracle@myserver02 (LGWR) 26593 /devices/diska3
```

For another example of the `lsod` command, see [Example 2](#).

md_backup

Purpose

The `md_backup` command creates a backup file containing metadata for one or more disk groups.

Syntax and Description

```
md_backup backup_file
          [-G 'diskgroup [,diskgroup,...]']
```

[Table 52](#) describes the options for the `md_backup` command.

Table 52 Options for the `md_backup` command

Option	Description
<i>backup_file</i>	Specifies the backup file in which you want to store the metadata.
<code>-G <i>diskgroup</i></code>	Specifies the disk group name of the disk group that must be backed up

By default all the mounted disk groups are included in the backup file, which is saved in the current working directory if a path is not specified with the file name.

Oracle Automatic Storage Management Cluster File System (Oracle ACFS) file system and Oracle ASM Dynamic Volume Manager(Oracle ADVM) volume information is not backed up.

Example

The first example shows the use of the `backup` command when run without the disk group option. This example backs up all the mounted disk groups and creates the backup image in the `/scratch/backup/allldgs20100422` file. The second example

creates a backup of the data disk group. The metadata backup that this example creates is saved in the `/scratch/backup/data20100422` file.

Example 61 Using the ASMCMD `md_backup` command

```
ASMCMD [+] > md_backup /scratch/backup/alldgs20100422
Disk group metadata to be backed up: DATA
Disk group metadata to be backed up: FRA
Current alias directory path: ORCL/ONLINELOG
Current alias directory path: ORCL/PARAMETERFILE
Current alias directory path: ORCL
Current alias directory path: ASM
Current alias directory path: ORCL/DATAFILE
Current alias directory path: ORCL/CONTROLFILE
Current alias directory path: ASM/ASMPARAMETERFILE
Current alias directory path: ORCL/TEMPFILE
Current alias directory path: ORCL/ARCHIVELOG/2010_04_20
Current alias directory path: ORCL
Current alias directory path: ORCL/BACKUPSET/2010_04_21
Current alias directory path: ORCL/ARCHIVELOG/2010_04_19
Current alias directory path: ORCL/BACKUPSET/2010_04_22
Current alias directory path: ORCL/ONLINELOG
Current alias directory path: ORCL/BACKUPSET/2010_04_20
Current alias directory path: ORCL/ARCHIVELOG
Current alias directory path: ORCL/BACKUPSET
Current alias directory path: ORCL/ARCHIVELOG/2010_04_22
Current alias directory path: ORCL/DATAFILE
Current alias directory path: ORCL/CONTROLFILE
Current alias directory path: ORCL/ARCHIVELOG/2010_04_21

ASMCMD [+] > md_backup /scratch/backup/data20100422 -G data
Disk group metadata to be backed up: DATA
Current alias directory path: ORCL/ONLINELOG
Current alias directory path: ASM
Current alias directory path: ORCL/CONTROLFILE
Current alias directory path: ASM/ASMPARAMETERFILE
Current alias directory path: ORCL/PARAMETERFILE
Current alias directory path: ORCL
Current alias directory path: ORCL/DATAFILE
Current alias directory path: ORCL/TEMPFILE
```

md_restore

Purpose

The `md_restore` command restores disk groups from a metadata backup file.

Syntax and Description

```
md_restore backup_file [--silent]
      [--full|--nodg|--newdg -o 'old_diskgroup:new_diskgroup [...]]
      [-S sql_script_file] [-G 'diskgroup [,diskgroup...]]
```

Table 53 describes the options for the `md_restore` command.

Table 53 Options for the `md_restore` command

Option	Description
<code>backup_file</code>	Reads the metadata information from <code>backup_file</code> .
<code>--silent</code>	Ignore errors. Typically, if <code>md_restore</code> encounters an error, it stops. Specifying this flag ignores any errors.
<code>--full</code>	Specifies to create a disk group and restore metadata.

Option	Description
<code>--nodg</code>	Specifies to restore metadata only.
<code>--newdg -o <i>old_diskgroup:new_diskgroup</i></code>	Specifies to create a disk group with a different name when restoring metadata. The <code>-o</code> option is required with <code>--newdg</code> .
<code>-S <i>sql_script_file</i></code>	Write SQL commands to the specified SQL script file instead of executing the commands.
<code>-G <i>diskgroup</i></code>	Select the disk groups to be restored. If no disk groups are defined, then all disk groups are restored.

Example

The first example restores the disk group data from the backup script and creates a copy. The second example takes an existing disk group data and restores its metadata. The third example restores disk group data completely but the new disk group that is created is named data2. The fourth example restores from the backup file after applying the overrides defined in the `override.sql` script file.

Example 62 Using the ASMCMD md_restore command

```

ASMCMD [+] > md_restore --full -G data --silent /scratch/backup/alldgs20100422
ASMCMD [+] > md_restore --nodg -G data --silent /scratch/backup/alldgs20100422
ASMCMD [+] > md_restore --newdg -o 'data:data2' --silent /scratch/backup/
data20100422
ASMCMD [+] > md_restore -S override.sql --silent /scratch/backup/data20100422
    
```

mkdg

Purpose

Creates a disk group based on an XML configuration file.

Syntax and Description

```
mkdg { config_file.xml | 'contents_of_xml_file' }
```

[Table 54](#) lists the syntax options for the `mkdg` command.

Table 54 Options for the mkdg command

Option	Description
<code><i>config_file</i></code>	Name of the XML file that contains the configuration for the new disk group. <code>mkdg</code> searches for the XML file in the directory where ASMCMD was started unless a path is specified. For examples of the valid tags and XML configuration file, see Example 63 and Example 64 .
<code><i>contents_of_xml_file</i></code>	The XML script enclosed in single quotations.

`mkdg` creates a new disk group with an XML configuration file that specifies the name of the disk group, redundancy, attributes, and paths of the disks that form the disk group. Redundancy is an optional parameter; the default is normal redundancy. For some types of redundancy, disks are required to be gathered into failure groups. In the

case that failure groups are not specified for a disk group, each disk in the disk group belongs to its own failure group.

The `mkdg` command only mounts a disk group on the local node.

It is possible to set some disk group attribute values during disk group creation. Some attributes, such as `AU_SIZE` and `SECTOR_SIZE`, can be set only during disk group creation. For more information about disk groups attributes, refer to “[Managing Disk Group Attributes](#)”.

The default disk group compatibility settings are 10.1 for Oracle ASM compatibility, 10.1 for database compatibility, and no value for Oracle ADVM compatibility. For information about disk group compatibility attributes, see “[Disk Group Compatibility](#)”.

[Example 63](#) shows the basic structure and the valid tags with their respective attributes for the `mkdg` XML configuration file.

Example 63 Tags for `mkdg` XML configuration file

```
<dg> disk group
      name          disk group name
      redundancy    normal, external, high

<fg> failure group
      name          failure group name
</fg>

<dsk> disk
      name          disk name
      string        disk path
      size          size of the disk to add
      force         true specifies to use the force option
</dsk>

<a>   attribute
      name          attribute name
      value         attribute value
</a>

</dg>
```

For information about altering a disk group with ASMCMD `chdg`, see “[chdg](#)”. For information about creating a disk group, see “[Creating Disk Groups](#)”.

Example

The following is an example of an XML configuration file for `mkdg`. The configuration file creates a disk group named `data` with `normal` redundancy. Two failure groups, `fg1` and `fg2`, are created, each with two disks identified by associated disk strings. The disk group compatibility attributes are all set to 11.2.

Example 64 `mkdg` sample XML configuration file

```
<dg name="data" redundancy="normal">
  <fg name="fg1">
    <dsk string="/dev/disk1" />
    <dsk string="/dev/disk2" />
  </fg>
  <fg name="fg2">
    <dsk string="/dev/disk3" />
    <dsk string="/dev/disk4" />
  </fg>
  <a name="compatible.asm" value="11.2" />
  <a name="compatible.rdbms" value="11.2" />
</dg>
```

```
<a name="compatible.advm" value="11.2"/>
</dg>
```

The following are examples of the `mkdg` command. The first example runs `mkdg` with an XML configuration file in the directory where ASMCMD was started. The second example runs `mkdg` using information on the command line.

Example 65 Using the ASMCMD `mkdg` command

```
ASMCMD [+] > mkdg data_config.xml
ASMCMD [+] > mkdg '<dg name="data"><dsk string="/dev/disk*"/></dg>'
```

mount

Purpose

Mounts a disk group.

Syntax and Description

```
mount [--restrict] { [-a] | [-f] diskgroup[ diskgroup ...] }
```

[Table 55](#) lists the syntax options for the `mount` command.

Table 55 Options for the `mount` command

Option	Description
<i>diskgroup</i>	Name of the disk group.
-a	Mounts all disk groups.
--restrict	Mounts in restricted mode.
-f	Forces the mount operation.

This operation mounts one or more disk groups. A disk group can be mounted with or without force or restricted options. For more information about mounting disk groups, see ["Mounting and Dismounting Disk Groups"](#).

Example

The following are examples of the `mount` command showing the use of the force, restrict, and all options.

Example 66 Using the ASMCMD `mount` command

```
ASMCMD [+] > mount -f data
ASMCMD [+] > mount --restrict data
ASMCMD [+] > mount -a
```

offline

Purpose

Offline disks or failure groups that belong to a disk group.

Syntax and Description

```
offline -G diskgroup
        { -F failgroup |-D disk}
        [-t {minutes | hours}]
```

Table 56 lists the syntax options for the `offline` command.

Table 56 Options for the offline command

Option	Description
-G <i>diskgroup</i>	Disk group name.
-F <i>failgroup</i>	Failure group name.
-D <i>disk</i>	Specifies a single disk name.
-t <i>minutes</i> <i>hours</i>	Specifies the time before the specified disk is dropped as <i>nm</i> or <i>nh</i> , where <i>m</i> specifies minutes and <i>h</i> specifies hours. For example, 120m or 2h. The default unit is hours.

When a failure group is specified, this implies all the disks that belong to it should be offline.

Example

The following are examples of the `offline` command. The first example offlines the `failgroup1` failure group of the data disk group. The second example offlines the `data_0001` disk of the data disk group with a time of 1.5 hours before the disk is dropped.

Example 67 Using the ASMCMD offline command

```
ASMCMD [+] > offline -G data -F failgroup1
ASMCMD [+] > offline -G data -D data_0001 -t 1.5h
```

online

Purpose

Online all disks, a single disk, or a failure group that belongs to a disk group.

Syntax and Description

```
online -G diskgroup { -a | -F failgroup |-D disk}
        [--power n] [-w]
```

Table 57 lists the syntax options for the `online` command.

Table 57 Options for the online command

Option	Description
-a	Online all offline disks in the disk group.
-G <i>diskgroup</i>	Disk group name.
-F <i>failgroup</i>	Failure group name.
-D <i>disk</i>	Disk name.

Option	Description
<code>--power n</code>	Specifies the power option (1 to 1024) which determines the level of resources for the disk resync and disk group rebalance. Larger values result in faster disk resync and disk group rebalance. The default is 1.
<code>-w</code>	Wait option. Causes ASMCMD to wait for the disk group to be rebalanced before returning control to the user. The default is not waiting.

When a failure group is specified, this implies all the disks that belong to it should be online.

Example

The following are examples of the `online` command. The first example online all disks in the `failgroup1` failure group of the data disk group with the `wait` option enabled. The second example online the `data_0001` disk in the data disk group.

Example 68 Using the ASMCMD online command

```
ASMCMD [+] > online -G data -F failgroup1 -w
```

```
ASMCMD [+] > online -G data -D data_0001
```

rebal

Purpose

Rebalances a disk group.

Syntax and Description

```
rebal [--power power] [-w] diskgroup
```

[Table 58](#) lists the syntax options for the `rebal` command.

Table 58 Options for the rebal command

Option	Description
<code>diskgroup</code>	Disk group name.
<code>--power power</code>	Power setting.
<code>-w</code>	Wait option. Causes ASMCMD to wait for the disk group to be rebalanced before returning control to the user. The default is not waiting.

The power level can be set to the same values as the `ASM_POWER_LIMIT` initialization parameter. A value of 0 disables rebalancing. If the rebalance power is not specified, the value defaults to the setting of the `ASM_POWER_LIMIT` initialization parameter. For information about the power level, see [“ASM_POWER_LIMIT”](#) and [“Tuning Rebalance Operations”](#).

You can determine if a rebalance operation is occurring with the ASMCMD `lsop` command. See [“lsop”](#). For more information about rebalancing a disk group, see [“Manually Rebalancing Disk Groups”](#).

Example

The following is an example of the `rebal` command that rebalances the `fra` disk group with a power level set to 4.

Example 69 Using the ASMCMD rebal command

```
ASMCMD [+] > rebal --power 4 fra

ASMCMD [+] > lsop
Group_Name Dsk_Num State Power
FRA        REBAL  RUN    4
```

remap

Purpose

Marks a range of blocks as unusable on the disk and relocates any data allocated in that range.

Syntax and Description

```
remap diskgroup disk block_range
```

[Table 59](#) lists the syntax options for the `remap` command.

Table 59 Options for the remap command

Option	Description
<i>diskgroup</i>	Disk group name in which a disk must have data relocated.
<i>disk</i>	Name of the disk that must have data relocated. The name must match the <code>NAME</code> column in the <code>V\$ASM_DISK</code> view.
<i>block_range</i>	Range of physical blocks to relocate in the format <i>start_range_number-end_range_number</i> .

The `remap` command only relocates blocks. It does not correct or repair blocks that contain corrupted contents. The command uses a physical block size based on the `SECTOR_SIZE` disk group attribute.

Examples

The first example remaps blocks 5000 through 5999 for disk `DATA_0001` in disk group `DATA`. The second example remaps blocks 6230 through 6339 for disk `FRA_0002` in disk group `FRA`.

Example 70 Using the ASMCMD remap command

```
ASMCMD [+] > remap DATA DATA_0001 5000-5999

ASMCMD [+] > remap FRA FRA_0002 6230-6339
```

setattr

Purpose

Sets the attributes for an Oracle ASM disk group.

Syntax and Description

```
setattr -G diskgroup attribute_name attribute_value
```

Table 60 lists the syntax options for the `setattr` command.

Table 60 Options for the `setattr` command

Option	Description
<code>-G <i>diskgroup</i></code>	Disk group name.
<code><i>attribute_name</i></code>	Name of the attribute.
<code><i>attribute_value</i></code>	Value of the attribute.

The `COMPATIBLE.ASM` attribute must be advanced before advancing other disk group compatibility attributes and its value must be greater than or equal to the value of other disk group compatibility attributes.

For information about disk group attributes, see [“Managing Disk Group Attributes”](#).

Example

The following are examples of the `setattr` command. The first example sets the disk group attribute `COMPATIBLE.ASM` to `12.1.0.2` for the `data` disk group. The second example sets the disk group attribute `COMPATIBLE.RDBMS` to `12.1` for the `data` disk group.

Example 71 Using the ASMCMD `setattr` command

```
ASMCMD [+] > setattr -G data compatible.asm 12.1.0.2
```

```
ASMCMD [+] > setattr -G data compatible.rdbms 12.1
```

umount

Purpose

Dismounts a disk group.

Syntax and Description

```
umount { -a | [-f] diskgroup }
```

Table 61 lists the syntax options for the `umount` command.

Table 61 Options for the `umount` command

Option	Description
<code><i>diskgroup</i></code>	Name of the disk group.
<code>-a</code>	Dismounts all mounted disk groups. These disk groups are listed in the output of the <code>V\$ASM_DISKGROUP</code> view.
<code>-f</code>	Forces the dismount operation.

Example

The following are examples of the `umount` command. The first example dismounts all disk groups mounted on the Oracle ASM instance. The second example forces the dismount of the `data` disk group.

Example 72 Using the ASMCMD umount command

```
ASMCMD [+] > umount -a
ASMCMD [+] > umount -f data
```

ASMCMD Template Management Commands

This section describes the ASMCMD template management commands. [page 10-64](#) provides a summary of the template management commands.

Command	Description
chtmpl	Changes the attributes of a template.
lstmpl	Lists disk group templates.
mktmpl	Adds a template to a disk group.
rmtmpl	Removes a template from a disk group.

chtmpl

Purpose

Changes the attributes of a template.

Syntax and Description

```
chtmpl -G diskgroup { [--striping {coarse|fine}]
  [--redundancy {high|mirror|unprotected} ] [--primary {hot|cold}]
  [--secondary {hot|cold}]} template
```

[Table 63](#) lists the syntax options for the `chtmpl` command.

Table 63 Options for the `chtmpl` command

Option	Description
<code>-G <i>diskgroup</i></code>	Name of the disk group.
<code><i>template</i></code>	Name of the template to change.
<code>--striping {coarse fine}</code>	Striping specification, either coarse or fine.
<code>--redundancy { high mirror unprotected}</code>	Redundancy specification, either high, mirror, or unprotected.
<code>--primary {hot cold}</code>	Intelligent Data Placement specification for primary extents, either hot or cold region.
<code>--secondary {hot cold}</code>	Intelligent Data Placement specification for secondary extents, either hot or cold region.

At least one of the following options is required: `--striping`, `--redundancy`, `--primary`, or `--secondary`.

For information about updating templates, see [“Modifying a Disk Group Template”](#).

Example

The following is an example of the `chtml` command that updates the `mytemplate` template of the `data` disk group. The redundancy attribute is set to high and the striping attribute is set to fine.

Example 73 Using the ASMCMD `chtml` command

```
ASMCMD [+] > chtml -G data --redundancy high --striping fine mytemplate
```

lstmpl

Purpose

Lists all templates for all disk groups or the templates for a specified disk group.

Syntax and Description

```
lstmpl [--suppressheader] [-l] [-G diskgroup] [pattern]
```

[Table 64](#) lists the syntax options for the `lstmpl` command.

Table 64 Options for the `lstmpl` command

Option	Description
<code>-G <i>diskgroup</i></code>	Specifies disk group name.
<code>--suppressheader</code>	Suppresses column headings.
<code>-l</code>	Displays all details.
<code><i>pattern</i></code>	Displays the templates that match pattern expression.

For information about template attributes, see [“Template Attributes”](#).

Example

The following is an example of the `lstmpl` command. The example lists all details of the templates in the `data` disk group.

Example 74 Using the ASMCMD `lstmpl` command

```
ASMCMD [+] > lstmpl -l -G data
```

Group_Name	Group_Num	Name	Stripe	Sys	Redund	PriReg	MirrReg
DATA	1	ARCHIVELOG	COARSE	Y	MIRROR	COLD	COLD
DATA	1	ASMPARAMETERFILE	COARSE	Y	MIRROR	COLD	COLD
DATA	1	AUDIT_SPILLFILES	COARSE	Y	MIRROR	COLD	COLD
DATA	1	AUTOBACKUP	COARSE	Y	MIRROR	COLD	COLD
DATA	1	AUTOLOGIN_KEY_STORE	COARSE	Y	MIRROR	COLD	COLD
DATA	1	BACKUPSET	COARSE	Y	MIRROR	COLD	COLD
DATA	1	CHANGETRACKING	COARSE	Y	MIRROR	COLD	COLD
DATA	1	CONTROLFILE	FINE	Y	HIGH	COLD	COLD
DATA	1	DATAFILE	COARSE	Y	MIRROR	COLD	COLD
DATA	1	DATAGUARDCONFIG	COARSE	Y	MIRROR	COLD	COLD
DATA	1	DUMPSET	COARSE	Y	MIRROR	COLD	COLD
DATA	1	FLASHBACK	COARSE	Y	MIRROR	COLD	COLD
DATA	1	FLASHFILE	COARSE	Y	MIRROR	COLD	COLD
DATA	1	INCR_XTRANSPORT BACKUPSET	COARSE	Y	MIRROR	COLD	COLD
DATA	1	KEY_STORE	COARSE	Y	MIRROR	COLD	COLD
DATA	1	OCRFILE	COARSE	Y	MIRROR	COLD	COLD
DATA	1	ONLINELOG	COARSE	Y	MIRROR	COLD	COLD
DATA	1	PARAMETERFILE	COARSE	Y	MIRROR	COLD	COLD
DATA	1	TEMPFILE	COARSE	Y	MIRROR	COLD	COLD

DATA	1	VOTINGFILE	COARSE	Y	MIRROR	COLD	COLD
DATA	1	XTRANSPORT	COARSE	Y	MIRROR	COLD	COLD
DATA	1	XTRANSPORT BACKUPSET	COARSE	Y	MIRROR	COLD	COLD

mktmpl

Purpose

Adds a template to a disk group.

Syntax and Description

```
mktmpl -G diskgroup [--striping {coarse|fine}]
      [--redundancy {high|mirror|unprotected} ] [--primary {hot|cold}]
      [--secondary {hot|cold}] template
```

[Table 65](#) lists the syntax options for the mktmpl command.

Table 65 Options for the mktmpl command

Option	Description
<i>-G diskgroup</i>	Name of the disk group.
<i>template</i>	Name of the template to create.
<i>--striping {coarse fine}</i>	Striping specification, either coarse or fine.
<i>--redundancy { high mirror unprotected}</i>	Redundancy specification, either high, mirror, or unprotected.
<i>--primary { hot cold }</i>	Intelligent Data Placement specification for primary extents, either hot or cold region.
<i>--secondary { hot cold }</i>	Intelligent Data Placement specification for secondary extents, either hot or cold region.

For information about adding templates, see [“Adding Templates to a Disk Group”](#).

Example

The following is an example of the mktmpl command that adds the mytemplate template to the data disk group. The new template has the redundancy set to mirror and the striping set to coarse.

Example 75 Using the ASMCMD mktmpl command

```
ASMCMD [+] > mktmpl -G data --redundancy mirror --striping coarse mytemplate
```

rmtmpl

Purpose

Removes a template from a disk group.

Syntax and Description

```
rmtmpl -G diskgroup template
```

[Table 66](#) lists the syntax options for the rmtmpl command.

Table 66 Options for the `rmtmpl` command

Option	Description
<code>-G diskgroup</code>	Name of the disk group.
<code>template</code>	Name of the template to delete.

For information about template attributes, see [“Template Attributes”](#).

Example

The following is an example of the `rmtmpl` command that removes the `mytemplate` template from the `data` disk group.

Example 76 Using the ASMCMD `rmtmpl` command

```
ASMCMD [+] > rmtmpl -G data mytemplate
```

ASMCMD File Access Control Commands

This section describes the ASMCMD Oracle ASM File Access Control commands. For information about Oracle ASM File Access Control, see [“Managing Oracle ASM File Access Control for Disk Groups”](#).

When administering users with ASMCMD, the users must be existing operating system users and their user names must have corresponding operating system user IDs. However, only users in the same cluster as the Oracle ASM instance can be validated.

Note:

When modifying ownership of files, the previous owner of a file cannot be dropped while the file is still open even after the ownership of the file has changed.

[page 10-67](#) provides a summary of ASMCMD Oracle ASM File Access Control commands.

Command	Description
chgrp	Changes the user group of a file or list of files.
chmod	Changes permissions of a file or list of files.
chown	Changes the owner of a file or list of files.
groups	Lists the user groups to which a user belongs.
grpmod	Adds or removes users from an existing user group.
lsgrp	Lists user groups.
lsusr	Lists users in a disk group.
mkgrp	Creates a new user group.
mkusr	Adds a user to disk group.
passwd	Changes the password of a user.

Command	Description
rmgrp	Deletes a user group.
rmusr	Deletes a user from a disk group.
rpusr	Replaces one a user with another in a disk group.

chgrp

Purpose

Changes the user group of a file or list of files.

Syntax and Description

```
chgrp usergroup file [file ...]
```

[Table 68](#) lists the syntax options for the `chgrp` command.

Table 68 Options for the `chgrp` command

Option	Description
<i>usergroup</i>	Name of the user group.
<i>file</i>	Name of a file.

Only the file owner or the Oracle ASM administrator can use this command. If the user is the file owner, then the user must also be either the owner or a member of the group for this command to succeed.

This command accepts a file name or multiple file names separated by spaces.

If you change the user group settings of an open file, then the operation currently running on the file completes using the old user group settings. The new settings take effect when re-authentication is required.

Examples

The following are examples of the `chgrp` command that change the Oracle ASM user group of the specified files.

Example 77 Using the ASMCMD `chgrp` command

```
ASMCMD [+] > chgrp asm_data +data/orcl/controlfile/Current.260.684924747
```

```
ASMCMD [+fra/orcl/archivelog/flashback] > chgrp asm_fra log_7.264.684968167 log_8.265.684972027
```

chmod

Purpose

Changes permissions of a file or list of files.

Syntax and Description

```
chmod mode file [file ...]
```

mode can be one of the following forms:

- { u g o | u g | u o | g o | u | g | o | a } { + | - } { r | w | r w }
 a specifies permissions for all users, u specifies permissions for the owner of the file, g specifies the group permissions, and o specifies permissions for other users.
- { 0 | 4 | 6 } { 0 | 4 | 6 } { 0 | 4 | 6 }
 The first digit specifies owner permissions, the second digit specifies group permissions, and the third digit specifies other permissions.

Table 69 lists the syntax options for the chmod command.

Table 69 Options for the chmod command

Option	Description
6	Read write permissions
4	Read only permissions
0	No permissions
u	Owner permissions, used with r or w
g	Group permissions, used with r or w
o	Other user permissions, used with r or w
a	All user permissions, used with r or w
+	Add a permission, used with r or w
-	Removes a permission, used with r or w
r	Read permission
w	Write permission
<i>file</i>	Name of a file

This command accepts a file name or multiple file names separated by spaces.

You can only set file permissions to read-write, read-only, and no permissions. You cannot set file permissions to write-only.

If you change the permission settings of an open file, then the operation currently running on the file completes using the old permission settings. The new settings take effect when re-authentication is required.

To view the permissions on a file, use the ASMCMD ls command with the --permission option. See "ls".

Examples

The following are examples of the chmod command that change the permissions of the specified files.

Example 78 Using the ASMCMD chmod command

```

ASMCMD [+fra/orcl/archivelog/flashback] > chmod ug+rw log_7.264.684968167 log_8.265.684972027

ASMCMD [+fra/orcl/archivelog/flashback] > chmod 640 log_7.264.684968167 log_8.265.684972027

ASMCMD [+] > ls --permission +fra/orcl/archivelog/flashback
User      Group      Permission  Name
grid      asm_fra    rw-r----- log_7.264.684968167
grid      asm_fra    rw-r----- log_8.265.684972027
    
```

chown

Purpose

Changes the owner of a file or list of files.

Syntax and Description

```
chown user[:usergroup ] file [file ...]
```

[Table 70](#) lists the syntax options for the `chown` command.

Table 70 Options for the `chown` command

Option	Description
<i>user</i>	The name of the user that becomes the new owner.
<i>usergroup</i>	Name of the user group to which the user belongs.
<i>file</i>	Name of a file.

user typically refers to the user that owns the database instance home. Oracle ASM File Access Control uses the operating system (OS) name to identify a database.

This command accepts a file name or multiple file names separated by spaces.

If you change the ownership settings of an open file, then the following applies:

- The operation currently running on the file completes using the old ownership and user group settings. The new settings take effect when re-authentication is required.
- The new owner of the file cannot be dropped from the disk group until all instances in a cluster are restarted in a rolling manner.

Only the Oracle ASM administrator can use this command.

Examples

The following are examples of the `chown` command that change the owner of the specified files to the `oracle1` operating system user.

Example 79 Using the ASMCMD `chown` command

```
ASMCMD [+fra/orcl/archivelog/flashback] > chown oracle1 log_7.264.684968167 log_8.265.684972027
```

```
ASMCMD [+fra/orcl/archivelog/flashback] > chown oracle1:asm_fra log_9.264.687650269
```

groups

Purpose

Lists all the user groups to which the specified user belongs.

Syntax and Description

```
groups diskgroup user
```

[Table 71](#) lists the syntax options for the `groups` command.

Table 71 Options for the groups command

Option	Description
<i>diskgroup</i>	Name of the disk group to which the user belongs.
<i>user</i>	Name of the user.

Examples

The following is an example of the `groups` command that displays the user groups of the data disk group to which the `oracle1` user belongs.

Example 80 Using the ASMCMD groups command

```
ASMCMD [+] > groups data oracle1
asm_data
```

grpmod**Purpose**

Adds or removes operating system (OS) users to and from an existing Oracle ASM user group.

Syntax and Description

```
grpmod { --add | --delete } diskgroup usergroup user [user...]
```

[Table 72](#) lists the syntax options for the `grpmod` command.

Table 72 Options for the grpmod command

Option	Description
<code>--add</code>	Specifies to add users to the user group.
<code>--delete</code>	Specifies to delete users from the user group.
<i>diskgroup</i>	Name of the disk group to which the user group belongs.
<i>usergroup</i>	Name of the user group.
<i>user</i>	Name of the user to add or remove from the user group.

Only the owner of the user group can use this command. The command requires the SYSASM privilege to run.

This command accepts an operating system user name or multiple user names separated by spaces. The operating system users are typically owners of a database instance home.

Examples

The following are examples of the `grpmod` command. The first example adds the `oracle1` and `oracle2` users to the `asm_fra` user group of the `fra` disk group. The second example removes the `oracle2` user from the `asm_data` user group of the data disk group.

Example 81 Using the ASMCMD grpmod command

```
ASMCMD [+] > grpmod --add fra asm_fra oracle1 oracle2
ASMCMD [+] > grpmod --delete data asm_data oracle2
```

lsgrp

Purpose

Lists all Oracle ASM user groups or only groups that match a specified pattern.

Syntax and Description

```
lsgrp [--suppressheader][-a] [ -G diskgroup ] [ pattern ]
```

Table 73 lists the syntax options for the lsgrp command.

Table 73 Options for the lsgrp command

Option	Description
--suppressheader	Suppresses column headings.
-a	Lists all columns.
-G <i>diskgroup</i>	Limits the results to the specified disk group name.
<i>pattern</i>	Displays the user groups that match the pattern expression.

Examples

The following are examples of the lsgrp command. The first example displays a subset of information about the user groups whose name matches the asm% pattern. The second example displays all information about all the user groups.

Example 82 Using the ASMCMD lsgrp command

```
ASMCMD [+] > lsgrp asm%
DG_Name Grp_Name Owner
FRA     asm_fra  grid
DATA    asm_data grid

ASMCMD [+] > lsgrp -a
DG_Name Grp_Name Owner Members
FRA     asm_fra  grid  oracle1
DATA    asm_data grid  oracle1 oracle2
```

lsusr

Purpose

Lists Oracle ASM users in a disk group.

Syntax and Description

```
lsusr [--suppressheader][-a] [-G diskgroup ] [ pattern ]
```

Table 74 lists the syntax options for the lsusr command.

Table 74 Options for the *lsusr* command

Option	Description
-a	List all users and the disk groups to which the users belong.
--suppressheader	Suppresses column headings.
-G <i>diskgroup</i>	Limits the results to the specified disk group name.
<i>pattern</i>	Displays the users that match the pattern expression.

Examples

The following is an example of the *lsusr* command. The example lists users in the data disk group and also shows the operating system Id assigned to the user.

Example 83 Using the ASMCMD *lsusr* command

```
ASMCMD [+] > lsusr -G data
User_Num OS_ID OS_Name
3        1001  grid
1        1021  oracle1
2        1022  oracle2
```

mkgrp

Purpose

Creates a new Oracle ASM user group.

Syntax and Description

```
mkgrp diskgroup usergroup [user] [user...]
```

[Table 75](#) lists the syntax options for the *mkgrp* command.

Table 75 Options for the *mkgrp* command

Option	Description
<i>diskgroup</i>	Name of the disk group to which the user group is added.
<i>usergroup</i>	Name of the user group to add. 30 is the maximum number of characters.
<i>user</i>	Name of the database user to add to the user group.

You can optionally specify a list of users to be included as members of the new user group.

Examples

The following is an example of the *mkgrp* command. This example creates the *asm_data* user group in the data disk group and adds the *oracle1* and *oracle2* users to the user group.

Example 84 Using the ASMCMD *mkgrp* command

```
ASMCMD [+] > mkgrp data asm_data oracle1 oracle2
```

mkusr

Purpose

Adds an operating system (OS) user to a disk group.

Syntax and Description

```
mkusr diskgroup user
```

[Table 76](#) lists the syntax options for the `mkusr` command.

Table 76 Options for the `mkusr` command

Option	Description
<i>diskgroup</i>	Specifies the name of the disk group to which the user is to be added.
<i>user</i>	Name of the user to add.

The user to be added must be a valid operating system user. Only a user authenticated as SYSASM can run this command.

Examples

The following are examples of the `mkusr` command. The first example adds the `oracle1` user to the `data` disk group. The second example adds the `oracle2` user to the `fra` disk group.

Example 85 Using the ASMCMD `mkusr` command

```
ASMCMD [+] > mkusr data oracle1
```

```
ASMCMD [+] > mkusr fra oracle2
```

passwd

Purpose

Changes the password of a user.

Syntax and Description

```
passwd user
```

[Table 77](#) lists the syntax options for the `passwd` command.

Table 77 Options for the `passwd` command

Option	Description
<i>user</i>	Name of the user.

An error is raised if the user does not exist in the Oracle ASM password file. The user is first prompted for the current password, then the new password. The command requires the SYSASM privilege to run.

Examples

The following is an example of the `passwd` command that changes the password of the `oracle2` user.

Example 86 Using the ASMCMD passwd command

```
ASMCMD [+] > passwd oracle2
Enter old password (optional):
Enter new password: *****
```

rmgrp

Purpose

Removes a user group from a disk group.

Syntax and Description

```
rmgrp diskgroup usergroup
```

[Table 78](#) lists the syntax options for the `rmgrp` command.

Table 78 Options for the `rmgrp` command

Option	Description
<i>diskgroup</i>	Name of the disk group to which the user group belongs.
<i>usergroup</i>	Name of the user group to delete.

Removing a group might leave some files without a valid user group. To ensure that those files have a valid group, explicitly update those files to a valid user group. See [“chgrp”](#).

The command must be run by the owner of the user group and also requires the SYSASM privilege to run.

Examples

The following is an example of the `rmgrp` command that removes the `asm_data` user group from the `data` disk group.

Example 87 Using the ASMCMD rmgrp command

```
ASMCMD [+] > rmgrp data asm_data
```

rmusr

Purpose

Deletes an operating system (OS) user from a disk group.

Syntax and Description

```
rmusr [-r] diskgroup user
```

[Table 79](#) lists the syntax options for the `rmusr` command.

Table 79 Options for the *rmusr* command

Option	Description
<i>-r</i>	Removes all files in the disk group that the user owns at the same time that the user is removed.
<i>diskgroup</i>	Specifies the name of the disk group from which the user is to be deleted.
<i>user</i>	Name of the user to delete.

The command requires the SYSASM privilege to run.

Examples

The following is an example of the *rmusr* command that removes the *oracle2* user from the data disk group.

Example 88 Using the ASMCMD *rmusr* command

```
ASMCMD [+] > rmusr data oracle2
```

rpusr

Purpose

Replaces one operating system (OS) user with another in a disk group.

Syntax and Description

```
rpusr diskgroup user1 user2
```

[Table 80](#) lists the syntax options for the *rpusr* command.

Table 80 Options for the *rpusr* command

Option	Description
<i>diskgroup</i>	Specifies the name of the disk group.
<i>user1</i>	Name of the user to be replaced.
<i>user2</i>	Name of user that replaces the existing user in the disk group.

The *rpusr* command replaces one operating system user with another in an Oracle ASM disk group. The replacement user must not be a user currently in the disk group user list.

If the command succeeds, all files that were previously owned by current user are now owned by the replacement user. The current user is automatically removed from the user list of the disk group. Adding the current user back to the disk group is possible but this user will not own any files.

When changing the ownership of an open file, the new owner cannot be dropped with the owner's files until all instances within a cluster are restarted.

The command requires the SYSASM privilege to run.

Examples

The following is an example of the *rpusr* command that replaces the *oracle1* user with the *oracle2* user in the data disk group.

Example 89 Using the ASMCMD rpusr command

```
ASMCMD [+] > rpusr data oracle1 oracle2
```


Part III

Oracle Automatic Storage Management Cluster File System

Part III discusses Oracle Automatic Storage Management Cluster File System (Oracle ACFS) and Oracle ASM Dynamic Volume Manager (Oracle ADVM), in the following chapters:

- [Introducing Oracle ACFS and Oracle ADVM](#)
- [Using Views to Display Oracle ACFS Information](#)
- [Administering Oracle ACFS with Oracle Enterprise Manager](#)
- [Managing Oracle ACFS and Oracle ADVM With ASMCA](#)
- [Managing Oracle ADVM with ASMCMD](#)
- [Managing Oracle ACFS with Command-Line Tools](#)

Introducing Oracle ACFS and Oracle ADVM

This chapter describes the components of Oracle Automatic Storage Management Cluster File System (Oracle ACFS) and Oracle ASM Dynamic Volume Manager (Oracle ADVM).

This chapter provides concepts and an overview of Oracle ACFS and Oracle ADVM features with the following topics:

- [Overview of Oracle ACFS](#)
- [Understanding Oracle ACFS Concepts](#)
- [Understanding Oracle ACFS Administration](#)
- [Overview of Oracle ASM Dynamic Volume Manager](#)

See Also:

- [“Managing Oracle ADVM Volumes in a Disk Group”](#) for information about using SQL*Plus to administer volumes
 - [“Features Enabled By Disk Group Compatibility Attribute Settings”](#) for information about Oracle ACFS features and disk group attribute settings
 - [Managing Oracle ASM With ASMCA](#) for information about using Oracle ASM Configuration Assistant to administer Oracle ACFS
 - [Using Views to Display Oracle ACFS Information](#) for information about using views to obtain Oracle ACFS information
 - [Managing Oracle ADVM with ASMCMD](#) for information about volume management commands
 - [Managing Oracle ACFS with Command-Line Tools](#) for information about Oracle ACFS operating system utilities
-

Overview of Oracle ACFS

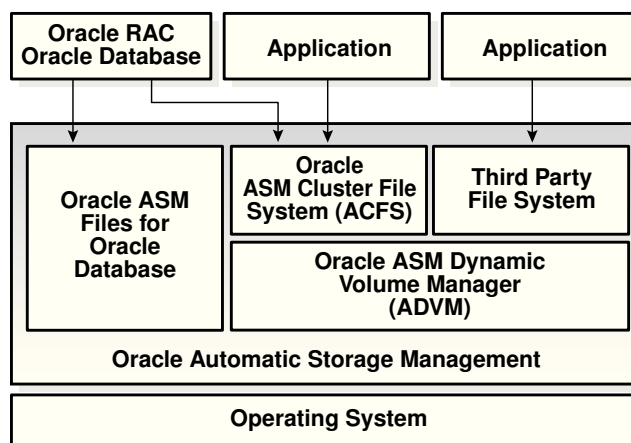
Oracle Automatic Storage Management Cluster File System (Oracle ACFS) is a multi-platform, scalable file system, and storage management technology that extends Oracle Automatic Storage Management (Oracle ASM) functionality to support all customer files. Oracle ACFS supports Oracle Database files and application files, including executables, database data files, database trace files, database alert logs, application reports, BFILEs, and configuration files. Other supported files are video, audio, text, images, engineering drawings, and all other general-purpose application

file data. Oracle ACFS conforms to POSIX standards for Linux and UNIX, and to Windows standards for Windows.

An Oracle ACFS file system communicates with Oracle ASM and is configured with Oracle ASM storage, as shown in [Figure 1](#) . Oracle ACFS leverages Oracle ASM functionality that enables:

- Oracle ACFS dynamic file system resizing
- Maximized performance through direct access to Oracle ASM disk group storage
- Balanced distribution of Oracle ACFS across Oracle ASM disk group storage for increased I/O parallelism
- Data reliability through Oracle ASM mirroring protection mechanisms

Figure 1 Oracle Automatic Storage Management Storage Layers



Oracle ACFS establishes and maintains communication with the Oracle ASM instance to participate in Oracle ASM state transitions including Oracle ASM instance and disk group status updates and disk group rebalancing. Oracle Automatic Storage Management with Oracle ACFS and Oracle ASM Dynamic Volume Manager (Oracle ADVM) delivers support for all customer data and presents a common set of Oracle storage management tools and services across multiple vendor platforms and operating system environments on both Oracle Restart (standalone) and cluster configurations. For an overview of Oracle ADVM, see [“Overview of Oracle ASM Dynamic Volume Manager”](#).

Oracle ACFS is tightly coupled with Oracle Clusterware technology, participating directly in Clusterware cluster membership state transitions and in Oracle Clusterware resource-based high availability (HA) management. In addition, Oracle installation, configuration, verification, and management tools have been updated to support Oracle ACFS.

Oracle ACFS can be accessed and managed using native operating system file system tools and standard application programming interfaces (APIs). Oracle ACFS can also be managed with Oracle ASM Configuration Assistant. Oracle ACFS can be accessed using industry standard Network Attached Storage (NAS) File Access Protocols: Network File System (NFS) and Common Internet File System (CIFS). However, CIFS clients on Windows cannot use ACLs when interfacing with Oracle ACFS Linux, Solaris, or AIX servers, but can use ACLs with Oracle ACFS on Windows.

In addition to sharing file data, Oracle ACFS provides additional storage management services including support for the Oracle Grid Infrastructure clusterwide mount

registry, dynamic online file system resizing, and multiple space efficient snapshots for each file system.

Oracle ACFS contributes to the overall Oracle storage management by providing:

- A general-purpose standalone server and cluster file system solution that is integrated with Oracle ASM and Oracle Clusterware technologies
- A common set of file system features across multiple vendor platforms and operating systems, offering an alternative to native operating system or third-party file system solutions
- Standalone and clusterwide shared Oracle Database homes, all Oracle Database files, and application data
- Uniform, coherent shared file access and clusterwide naming of all customer application files
- Integration with Oracle Clusterware High Availability Resources

For more information, refer to [“Oracle Clusterware Resources and Oracle ACFS Administration”](#)

Oracle ACFS accommodates large storage capacities and large numbers of cluster nodes. It efficiently manages large numbers of file systems, files, and supports both small and large sized files with exabyte-capable file and file system capacities. Oracle ACFS provides optimized fast directory lookup for large directories with millions of files.

Oracle ACFS file systems are generally mounted on all Oracle Cluster Synchronization Services (CSS) cluster members. In the event of a member failure, another cluster member quickly recovers any outstanding metadata transactions on behalf of the failed member. Following recovery, access by other active cluster members and any remote client systems can resume.

The following list provides important information about Oracle ACFS:

- For all applications, Oracle ACFS performance is best with larger write() sizes, such as 8 K or larger.
- For best performance, use the Deadline I/O Scheduler for the disks in the disk group on a Linux system.
- When creating Oracle ACFS file systems on Windows, log on as a Windows domain user. Also, when creating files in an Oracle ACFS file system on Windows, you should be logged in as a Windows domain user to ensure that the files are accessible by all nodes.
- When using a file system across cluster nodes on Windows platforms, the best practice is to mount the file system using a domain user, to ensure that the security identifier is the same across cluster nodes. Windows security identifiers, which are used in defining access rights to files and directories, use information which identifies the user. Local users are only known in the context of the local node. Oracle ACFS uses this information during the first file system mount to set the default access rights to the file system.

Refer to the *Oracle Database Installation Guide* for the Windows platform for information about Oracle Base permissions when a file system is mounted under Oracle Base.

- Oracle ACFS does not support any files associated with the management of Oracle ASM, such as files in the Oracle Grid Infrastructure home and in the Oracle ASM diagnostic directory.
- Oracle ACFS does not support Oracle Cluster Registry (OCR) and voting files.
- Oracle ACFS functionality requires that the disk group compatibility attributes for ASM and ADVM be set to 11.2 or higher. For information about disk group compatibility, refer to [“Disk Group Compatibility”](#).
- To use an Oracle ACFS file system for an Oracle Database home, the release level must be Oracle 11g Release 2 (11.2) or later.

For information about managing and monitoring Oracle ACFS, refer to [Managing Oracle ACFS with Command-Line Tools](#) and [Using Views to Display Oracle ACFS Information](#).

Understanding Oracle ACFS Concepts

This section describes concepts for the key Oracle ACFS components and contains the following topics:

- [About Oracle ACFS](#)
- [About the Oracle ACFS Mount Model and Namespace](#)
- [About Oracle ACFS and Database Data Files](#)
- [About Oracle ACFS and Oracle Database Homes](#)
- [About Oracle ASM Dynamic Volume Manager](#)
- [About the Oracle ACFS Driver Model](#)
- [About the Oracle ACFS Mount Registry](#)
- [About Oracle ACFS Snapshots](#)
- [About Oracle ACFS and Backup and Restore](#)
- [About Oracle ACFS Integration with Oracle ASM](#)
- [About Oracle ACFS and External Tables on Windows](#)

About Oracle ACFS

Oracle ACFS is designed as a general-purpose, standalone server and clusterwide file system that delivers support for all customer files. Users and applications can access and manage Oracle ACFS using native operating system file system application programming interfaces (APIs) and command-line interface (CLI) tools. Users can also manage Oracle ACFS with Oracle ASM Configuration Assistant (ASMCA).

Oracle ACFS supports large files with 64-bit file and file system data structure sizes leading to exabyte capable file and file system capacities on 64 bit platforms. Variable extent-based storage allocation and high-performance directories contribute to fast performance and shared disk configurations that provide direct storage paths to Oracle ACFS file data from each cluster member. File system integrity and fast recovery is achieved with Oracle ACFS metadata checksums and journaling. Oracle

ACFS is designed as a multi-node, shared file system model that delivers coherent, cached, direct storage paths to Oracle ACFS file data from each cluster member.

Oracle ACFS file systems are typically configured for clusterwide access. File systems, files, and directories are visible and accessible from all cluster members and can be referenced by users and applications using the same path names from any cluster member. This design enables simplified application deployments across cluster members and facilitates both multiple instance cluster applications and high availability (HA) failover of unmodified standalone server applications.

Oracle ACFS presents single system file access semantics across cluster configurations. Applications and users on all cluster members are always presented with the same view of shared Oracle ACFS file data, supported by the Oracle ACFS clusterwide user and metadata cache coherency mechanism.

About the Oracle ACFS Mount Model and Namespace

Oracle ACFS is designed as a hierarchical file system containing files and subdirectories organized into a tree-structured namespace with files at the leaves. The namespace design is a single-file system naming model for both standalone server and cluster configurations. This design enables each cluster member to present shared files to cluster applications using the same path names, simplifying multi-node application and user access, and overall file system administration. The Oracle ACFS mount model also accommodates node local mounts and cluster node subset mounts in cluster configurations to accommodate additional customer requirements.

It is best practice for Oracle ACFS file systems to be Oracle Clusterware managed with Oracle Clusterware resources to ensure they are properly handled during Oracle Grid Infrastructure startup and shutdown.

You can explicitly use the `mount` command. However, if the resource has been created, then the file system may already be mounted.

About Oracle ACFS and Database Data Files

Note:

The best practice for data files in Oracle ACFS is to use a clusterwide resource for the Oracle ACFS File system that stores the data files. For additional information, refer to [“Creating Oracle ACFS Resources”](#).

If the data files are added after the database installation is complete, you must modify the database dependencies to list the new Oracle ACFS file system. Failure to do so results in errors with application reliability. To specify the file systems in the dependency list, use the `SRVCTL` database object command to modify the Oracle ACFS paths used by the resource.

Oracle ACFS in Oracle Grid 12c Release 1 (12.1) supports all database files starting with Oracle Database 11g Release 2 (11.2.0.4), except for data files and redo logs in an Oracle Restart (standalone server) configuration. Oracle ACFS can be configured for use with the database particularly to leverage Oracle ACFS snapshots for database testing and development. To support database files, the `COMPATIBLE .ADVM` attribute must be set to 12 . 1 or higher for the disk group that contains the Oracle ACFS file system.

Support for database data files on Windows begins with Oracle Grid 12c Release 1 (12.1.0.2). For support of database files on Windows, the `COMPATIBLE.ADVM` attribute must be set to 12.1.0.2 or higher.

Support for database data files on Oracle Exadata (Linux) begins with Oracle Grid 12c Release 1 (12.1.0.2). However, Oracle ACFS does not currently have the ability to push database operations directly into storage.

Oracle ACFS additionally supports all database files for Oracle Database 10g Release 2 (10.2.0.4 and 10.2.0.5) on Oracle Exadata (Linux) storage only. For database file support with Oracle Database 10g Release 2 (10.2.0.4 and 10.2.0.5) on Oracle Exadata storage, the following conditions must be met:

- When creating an Oracle Database with DBCA, you must set the `REMOTE_LISTENER` initialization parameter to `your_scan_vip:1521` otherwise DBCA fails during the create process. For information about the `REMOTE_LISTENER` initialization parameter, refer to *Oracle Database Reference*.
- You must modify all the start and stop dependencies of the database instance resources to ensure that the resources start when starting Oracle Clusterware. For information about resource dependencies, refer to *Oracle Clusterware Administration and Deployment Guide*.

The following list provides important information about using Oracle ACFS with database files:

- Oracle ACFS support includes all file types supported by Oracle ASM. For a list of file types supported by Oracle ASM, refer to [Table 1](#).
- Oracle ACFS does not support data files or redo logs in an Oracle Restart configuration. Oracle ACFS does not support direct I/O in an Oracle Restart configuration.
- When storing database data files on Oracle ACFS, you must set the `FILESYSTEMIO_OPTIONS` initialization parameter to `setall`; other settings are not supported. To achieve optimal performance with database data files, set `ASM` and `ADVM` compatibility attributes to 12.1 or higher for the disk group that contains the Oracle `ADVM` volume intended to hold the data files. For volumes created before 12.1.0.2, set the stripe columns to 1, or set the stripe columns to 8 and the stripe width to 1 MB. Volumes created while running 12.1.0.2 or higher already default to the high performance configuration (stripe columns = 8 and stripe width = 1 MB). For information about creating a volume, refer to “[volcreate](#)”.
- To obtain optimal database performance with snapshots, the snapshots must be created after the `ADVM` compatibility attribute is set to 12.1 or higher.
- Use a 4 K or larger database block size and tablespace block size with Oracle ACFS for best performance.
- If a data file is configured to automatically extend, then the size of the increments should be large enough to ensure that the extend operation occurs infrequently. Frequent automatic extends have a negative performance impact.
- Running a workload in a snapshot reduces resources for the primary workload running on the base files because the storage is shared between the base file system and the snapshots. To run test scenarios in Oracle ACFS snapshots without impacting the primary workload, copy the file system and then run test workloads on snapshots created in the copied file system.

- Using Oracle ACFS replication or encryption with database files on Oracle ACFS is not supported. For information about other replication options for database files on Oracle ACFS, refer to *Oracle Data Guard Concepts and Administration* and Oracle GoldenGate documentation. Oracle GoldenGate is an Oracle product sold independently of the Oracle Database. To encrypt database data files on Oracle ACFS, Oracle recommends Oracle Advanced Security. Oracle Advanced Security provides Transparent Data Encryption (TDE) to encrypt data files for entire tablespaces. For information about Transparent Data Encryption (TDE), refer to *Oracle Database Advanced Security Guide*.

About Oracle ACFS and Oracle Database Homes

An Oracle ACFS file system can be configured as an Oracle Database home. When installing a database in a cluster, it is required to use a shared Oracle ACFS file system for the database home. You can use an Oracle ACFS file system for an Oracle Database home with Oracle 11g Release 2 (11.2) or later.

When installing Oracle Software, there must be a separate Oracle base (ORACLE_BASE) associated with each operating system user. For example, there should be a separate Oracle base for a grid user and a database user.

See Also:

Oracle Database Installation Guide for information about Optimal Flexible Architecture (OFA) recommendations for Oracle base and home directories

You can locate the Oracle Database base (ORACLE_BASE for database) directory and home (ORACLE_HOME for database) directory on an Oracle ACFS file system. The Oracle Database base (ORACLE_BASE for database) directory should not be the Oracle Grid Infrastructure base (ORACLE_BASE for grid) directory or should not be located under the Oracle Grid Infrastructure base directory (ORACLE_BASE for grid).

The Oracle Grid Infrastructure base (ORACLE_BASE for grid) directory and home (ORACLE_HOME for grid) directory cannot be located on the Oracle ACFS file system because the Oracle ACFS file system cannot be created until Oracle Grid Infrastructure is installed.

One or more Oracle Database homes on Oracle ACFS can be created under the same mount point with each home using a separate Oracle ACFS file system.

After the installation of Oracle Grid Infrastructure Software and before the installation of the Oracle Database software with Oracle Universal Installer (OUI), you can create an Oracle ACFS file system to be configured for use as an Oracle Database home.

You can also use the Oracle ASM Configuration Assistant (ASMCA) or Oracle ACFS commands to create the file system. For information about using ASMCA, refer to [“Creating an Oracle ACFS File System for Database Use”](#).

For information about using Oracle ACFS commands to create a file system, refer to [Managing Oracle ACFS with Command-Line Tools](#).

Note:

When an Oracle ACFS file system contains an Oracle Database home or Oracle Database uses the file system for any file storage, the file system must have an Oracle ACFS file system resource. If you have not used Oracle ASM Configuration Assistant to setup the mount point, then you must use Server Control Utility (SRVCTL) commands to set up Oracle Database dependencies. For information about SRVCTL, see *Oracle Real Application Clusters Administration and Deployment Guide*.

In an Oracle Grid Infrastructure clusterware configuration, a clusterwide Oracle ACFS resource is required when using Oracle ACFS for the database home. To enable the database owner to act on the resource, the owner must be specified as a permitted user when creating the resource. You can specify the database owner with the `-u` option of the `srvctl add filesystem` or `acfsutil registry` command. Root privilege is required when adding the resource in Linux or Unix environments. For additional information, refer to [“Creating Oracle ACFS Resources”](#).

After the Oracle ACFS file system and resources are created, the Oracle ACFS-based database home mount point location can be selected as the Oracle Database home location by browsing to and then choosing the directory during the Oracle Universal Installer (OUI) Database Software installation.

You can use the `srvctl start filesystem` command to manually mount the Oracle ACFS file system.

Note:

When additional Oracle ACFS file systems are added to an Oracle Database after creation, they must be specified in the Oracle Database Resource Dependency list. Failure to do so results in errors with application reliability. To specify the file systems in the dependency list, use the SRVCTL database object command to modify the Oracle ACFS paths used by the resource.

Oracle ACFS file systems can be also configured for use as a home for applications. However, Oracle ACFS file systems cannot be used for an Oracle base directory or an Oracle Grid Infrastructure home that contains the software for Oracle Clusterware, Oracle ASM, Oracle ACFS, and Oracle ADVM components.

To reduce contention on an Oracle ACFS file system in an Oracle RAC environment where the Oracle Database home is shared on Oracle ACFS, Oracle Database auditing operating system files should be configured as node specific. For a node-specific setup, you must ensure that the `AUDIT_FILE_DEST` initialization parameter in the configuration file of each database instance points to a unique location rather than one location for all the database instances.

For example, if you have a database with the Oracle name set to `TEST` and you want to ensure that the location of `AUDIT_FILE_DEST` initialization parameter for each database instance, such as `TEST1` or `TEST2`, points to a node specific location for that instance, you can run the following SQL statement:

```
SQL> ALTER SYSTEM SET AUDIT_FILE_DEST= '$ORACLE_BASE/admin/adump/TEST/@'
SCOPE=SPFILE SID= '* ' ;
```

In the previous example, @ expands to the ORACLE_SID of each instance. If ORACLE_BASE has been set to /acfsmounts in this example, then that value could have been used in place of the ORACLE_BASE variable.

See Also:

- *Oracle Database Installation Guide* for your environment for information about the installation of Oracle Database software and storage options
 - *Oracle Grid Infrastructure Installation Guide* for your environment for information about the installation of Oracle Grid Infrastructure software and storage options
 - *Oracle Database Administrator's Guide* for information about using Oracle Managed files
 - *Oracle Database Reference* for information about the AUDIT_FILE_DEST initialization parameter
-
-

About Oracle ASM Dynamic Volume Manager

The Oracle ASM Dynamic Volume Manager (Oracle ADVM) provides volume management services and a standard disk device driver interface to clients. File systems and other disk-based applications send I/O requests to Oracle ADVM volume devices as they would to other storage devices on a vendor operating system.

For more information about Oracle ADVM, refer to “[Overview of Oracle ASM Dynamic Volume Manager](#)”.

About the Oracle ACFS Driver Model

An Oracle ACFS file system is installed as a dynamically loadable vendor operating system (OS) file system driver and tool set that is developed for each supported operating system platform. The driver is implemented as a Virtual File System (VFS) and processes all file and directory operations directed to a specific file system.

Note:

Errors encountered by the drivers are written to the native operating system console and system event loggers. Refer to “[Understanding Oracle ACFS I/O Failure Console Messages](#)”.

About the Oracle ACFS Mount Registry

The Oracle ACFS mount registry supports Oracle Grid Infrastructure cluster configurations, but does not support Oracle Restart configurations. File systems that are to be mounted persistently (across restarts) can be registered with the Oracle ACFS mount registry. In cluster configurations, registered Oracle ACFS file systems are automatically mounted by the mount registry, similar to a clusterwide mount table. However, in Oracle Restart configurations the automatic mounting of registered Oracle ACFS file systems is not supported. For more information, see “[Oracle ACFS and Oracle Restart](#)”.

By default, an Oracle ACFS file system that is inserted into the Oracle ACFS mount registry is automatically mounted on all cluster members, including cluster members that are added after the registry addition. However, the Oracle ACFS mount registry also accommodates standalone and multi-node (subset of cluster nodes) file system registrations. The mount registry actions for each cluster member mount only registered file systems that have been designated for mounting on that member.

The Oracle ACFS mount registry is implemented using Oracle Clusterware resources, specifically the Oracle ACFS resource. The Oracle ACFS resource actions are designed to automatically mount a file system only one time for each Oracle Grid Infrastructure initialization to avoid potential conflicts with administrative actions to dismount a given file system.

For information about registering an Oracle ACFS file system using the `acfsutil` command, refer to [“acfsutil registry”](#) or the SRVCTL `srvctl add filesystem` command.

For more information about the implementation of the mount registry and Oracle ACFS resources, refer to [“Oracle Clusterware Resources and Oracle ACFS Administration”](#).

See Also:

- *Oracle Real Application Clusters Administration and Deployment Guide* for information about the SRVCTL `srvctl add filesystem` command and registering an Oracle ACFS file system
 - *Oracle Clusterware Administration and Deployment Guide* for information about Oracle Clusterware resources
-
-

About Oracle ACFS Snapshots

An Oracle ACFS snapshot is an online, read-only or read-write, point in time copy of an Oracle ACFS file system. The snapshot copy is space-efficient and uses Copy-On-Write functionality. Before an Oracle ACFS file extent is modified or deleted, its current value is copied to the snapshot to maintain the point-in-time view of the file system.

Oracle ACFS snapshots are immediately available for use after they are created. The snapshots are created in the `.ACFS/snaps/` directory of the file system. They are always online while the file system is mounted. Consequently, an Oracle ACFS snapshot can support the online recovery of files inadvertently modified or deleted from a file system. With up to a total of 1023 read-only, read-write, or combination of read-only and read-write snapshot views supported for each file system, flexible online file recovery solutions spanning multiple views can be employed. An Oracle ACFS snapshot can also be used as the source of a file system backup, as it can be created on demand to deliver a current, consistent, online view of an active file system. For information about the number of snapshots supported, refer to [“Oracle ACFS Disk Space Usage”](#).

Oracle ACFS read-write snapshots enable fast creation of an snapshot image that can be both read and written without impacting the state of the Oracle ACFS file system hosting the snapshot images. You can use read-write snapshots for:

- Testing of new versions of application software on production file data reflected in the read-write snapshot image without modifying the original production file system
- Running test scenarios on a real data set without modifying the original production file system

To use Oracle ACFS read-write snapshots, the disk group compatibility attribute for ADVM must be set to 11.2.0.3.0 or higher. If you create a read-write snapshot on an existing Oracle ACFS file system from a version earlier than 11.2.0.3.0, then the file system is updated to the 11.2.0.3.0 or higher format. After a file system has been updated to a higher version, an Oracle ACFS file system cannot be reverted to an earlier version, and accordingly cannot be mounted on an earlier Oracle Grid Infrastructure version.

You can create a snapshot from an existing snapshot in the same Oracle ACFS file system. In addition, you can convert a snapshot between read-only and read-write formats. To create from an existing snapshot or convert a snapshot, the disk group compatibility attribute for ADVM must be set to 12.1 or higher. In addition, creation from an existing snapshot is not permitted if there are:

- Any snapshots present in the file system that were created with the ADVM compatibility set to less than 12.1
- Any snapshots of the file system that were created after ADVM compatibility was set to 12.1 but while 11.2 snapshots existed

Oracle ACFS snapshot storage is maintained within the file system, eliminating the management of separate storage pools for file systems and snapshots. Oracle ACFS file systems can be dynamically resized to accommodate additional file and snapshot storage requirements.

You cannot modify security or encryption metadata in read-write snapshots except for enabling or disabling security or encryption. No other alteration is permitted on Oracle ACFS security or encryption metadata in a snapshot. If a file was not secured by a security realm in the snapshot, it cannot be realm secured by adding the corresponding file in the active file system to a security realm. If a file was not encrypted in the snapshot, that file cannot be encrypted by encrypting the corresponding file in the active file system.

A new file created in a realm-secured directory in a read-write snapshot inherits the realm security attributes of the parent directory. If the realm protecting the new file has encryption turned on, the file is encrypted with the encryption parameters set in the realm. If the realm protecting the new file has encryption turned off, the file is decrypted. Files and directories in a read-write snapshot cannot be added to or removed from any security realm.

Files in a read-write snapshot can be encrypted, decrypted, or rekeyed if the operation target is a path specified for a file or directory of the read-write snapshot. However, if an encryption, decryption, or rekey operation is specified at the file system level, then the operation does not process files and directories of snapshots in the `.ACFS/snaps/` directory.

All Oracle ACFS snapshot operations are serialized clusterwide in the kernel. For example, if a snapshot create operation is initiated at the same time as a snapshot delete operation, then both operations would complete, but they would not run in parallel inside of the kernel. One operation would complete before the other was started.

For information about Oracle ACFS security, refer to [“Oracle ACFS Security”](#).

For information about Oracle ACFS encryption, refer to “[Oracle ACFS Encryption](#)”.

Oracle ACFS snapshots are administered with the `acfsutil snap` commands. For information about the `acfsutil snap` commands, refer to “[acfsutil snap create](#)”, “[acfsutil snap delete](#)”, and “[acfsutil snap info](#)”.

Note:

The `link()` and `rename()` system calls fail if an attempt is made to link or rename a file in the Oracle ACFS file system and a file in any associated read-write snapshot, or vice versa. Any tools which use the `link()` and `rename()` system calls, such as `ln` and `mv`, also fail in the same scenario.

About Oracle ACFS and Backup and Restore

Oracle ACFS runs on operating system platforms as a native file system technology supporting native operating system file system application programming interfaces (APIs). Consequently, backup applications that access files using the native operating system file system interfaces are able to access and backup Oracle ACFS file systems and other native operating system file systems. Oracle ACFS snapshots can be dynamically created and used to present a consistent, on-line view of an active file system to a backup application.

Backup applications that use interfaces other than the standard operating system interfaces (read or write) are not supported with Oracle ACFS. For example, Windows backup applications that depend upon the presence of reparse points or the Windows Volume Shadow Copy Service (VSS) are not supported.

For information about using common operating system utilities to preserve Extend Attributes for tagging definitions, refer to “[Oracle ACFS Tagging](#)”.

About Oracle ACFS Integration with Oracle ASM

Oracle ACFS is always configured with Oracle ASM storage and interfaces with Oracle ASM storage through a traditional device file. This device file is presented by Oracle ADVM and is constructed using a dynamic volume file. The Oracle ADVM volume device file is created automatically following the creation of an Oracle ADVM volume. An Oracle ACFS file system is then bound to the Oracle ADVM device file during the file system creation.

After an Oracle ACFS is configured and mounted, the file system inherits the Oracle ASM storage management features associated with an Oracle ADVM volume, including dynamic balanced distribution, mirroring and striping, and dynamic resizing.

The Oracle ACFS driver establishes communication with the Oracle ASM instance to receive Oracle ASM status information including Oracle ASM instance and disk group state transitions. However, I/O does not go through Oracle ASM nor through the Oracle ASM proxy, but rather goes directly to the underlying Oracle ASM storage.

For information about Oracle ACFS and Oracle ASM operations, refer to “[Oracle ACFS and Dismount or Shutdown Operations](#)”.

About Oracle ACFS and External Tables on Windows

To access an external table stored on an Oracle ACFS file system on Windows, the external table must be created with the `DISABLE_DIRECTORY_LINK_CHECK` access parameter.

See Also:

- *Oracle Database Utilities* for information about the `DISABLE_DIRECTORY_LINK_CHECK` access parameter
 - *Oracle Database SQL Language Reference* for information about creating external tables
-
-

Understanding Oracle ACFS Administration

This section describes Oracle ACFS administration and contains the following topics:

- [Oracle ACFS and File Access and Administration Security](#)
- [Oracle ACFS and Grid Infrastructure Installation](#)
- [Oracle ACFS Configuration](#)
- [Oracle Clusterware Resources and Oracle ACFS Administration](#)
- [Oracle ACFS and Dismount or Shutdown Operations](#)
- [Oracle ACFS Security](#)
- [Oracle ACFS Encryption](#)
- [Oracle ACFS Auditing](#)
- [Oracle ACFS Replication](#)
- [Oracle ACFS Tagging](#)
- [Using Replication with Auditing_ Encryption_ and Security](#)
- [Oracle ACFS Plugins](#)
- [High Availability Network File Storage for Oracle Grid Infrastructure](#)

Oracle ACFS and File Access and Administration Security

Oracle ACFS supports both traditional Unix-style file access control classes (user, group, other) for Linux environments and the Windows Security Model including file access control lists (ACLs) for Windows platforms. Most Oracle ACFS administrative actions are performed by users with either root or Oracle ASM administration privileges for Linux environments and by users with Windows Administrative privileges on Windows platforms. General Oracle ACFS information for file systems can be accessed by any system user.

In support of Oracle ACFS administration, Oracle recommends that the Oracle ASM administrator role is given to a root privileged user, as many common Oracle ACFS

file system management tasks including mount, umount, fsck, driver load, and driver unload are root privileged operations. Other privileged Oracle ACFS file system operations that do not require root privileges can be performed by the Oracle ASM administrator. If the Oracle ASM administrator role is not given to a root privileged user, access to Oracle ACFS file systems can be restricted with the `norootsuid` and `nodev` mount options.

Additional fine grain access control is provided for Oracle ACFS file systems with the security infrastructure feature. For information about Oracle ACFS security infrastructure, refer to [“Oracle ACFS Security”](#).

For information about Oracle ACFS encryption, refer to [“Oracle ACFS Encryption”](#).

For information about Oracle ASM privileges, refer to [“About Privileges for Oracle ASM”](#).

For information about administering Oracle ACFS, refer to [Managing Oracle ACFS with Command-Line Tools](#).

Oracle ACFS and Grid Infrastructure Installation

Oracle Grid Infrastructure includes Oracle Clusterware, Oracle ASM, Oracle ACFS, Oracle ADVM, and driver resources software components, which are installed into the Grid Infrastructure home using the Oracle Universal Installation (OUI) tool.

Oracle ACFS Configuration

After a Grid Infrastructure installation and with an operational Oracle Clusterware, you can use Oracle ASM Configuration Assistant (ASMCA) to start the Oracle ASM instance and create Oracle ASM disk groups, Oracle ADVM volumes, and Oracle ACFS file systems. Alternatively, Oracle ASM disk groups and Oracle ADVM volumes can be created using SQL*Plus and ASMCMD command line tools. File systems can be created using operating system command-line tools.

Oracle ACFS file systems are configured with Oracle ADVM based operating system storage devices that are created automatically following the creation of an Oracle ADVM dynamic volume file. After a volume file and its associated volume device file are created, a file system can be created and bound to that operating system storage device. Following creation, an Oracle ACFS file system can be mounted, after which it is accessible to authorized users and applications executing file and file system operations.

For an example of the specific actions required to create a file system, refer to [“Basic Steps to Manage Oracle ACFS Systems”](#).

For information about managing Oracle ACFS file systems with ASMCA, refer to [“ASMCA GUI Tool for Managing Oracle ACFS and Oracle ADVM”](#).

For information about using Oracle ACFS commands to create a file system, refer to [Managing Oracle ACFS with Command-Line Tools](#).

For information about configuring Oracle Clusterware resources for use with the database, refer to [“Oracle Clusterware Resources and Oracle ACFS Administration”](#).

Oracle Clusterware Resources and Oracle ACFS Administration

Oracle Clusterware resources support all aspects of Oracle ACFS. The resources are responsible for enabling and disabling volumes, loading drivers and mounting and unmounting file systems.

This section discusses the following topics:

- [Summary of Oracle ACFS Resource-based Management](#)
- [High Availability Actions](#)
- [Creating Oracle ACFS Resources](#)
- [Node-Local or Clusterwide File Systems](#)
- [Monitoring Oracle ACFS resources](#)
- [Stopping Oracle ACFS resources](#)
- [Oracle ACFS resource Limitations](#)

Summary of Oracle ACFS Resource-based Management

The following list provides a summary of Oracle ACFS resource-based management.

- The Oracle ACFS, Oracle Kernel Services (OKS), and Oracle ADVM drivers are dynamically loaded when the Oracle ASM instance is started.
 - Oracle ACFS
This driver processes all Oracle ACFS file and directory operations.
 - Oracle ADVM
This driver provides block device services for Oracle ADVM volume files that are used by file systems for creating file systems.
 - Oracle Kernel Services Driver (OKS)
This driver provides portable driver services for memory allocation, synchronization primitives, and distributed locking services to Oracle ACFS and Oracle ADVM.

The drivers are managed as a single resource set. For additional information, see [“Oracle ACFS Drivers Resource Management”](#) and [“Oracle ACFS Driver Commands”](#).

- When a volume is created, Oracle ADVM creates a resource with the name of `ora.DISKGROUP.VOLUME.advm`. This resource is usually managed through transparent high availability calls from Oracle ASM and requires no user interaction. However, the user may choose to use the SRVCTL command interface to start and stop volumes as well as control the default state of the volume after an Oracle ASM restart. This is especially beneficial in a large cluster or an Oracle Flex ASM cluster, as volumes on other nodes may be operated upon.

In addition, these Oracle ADVM resources can be used by other resources in the Oracle Clusterware stack to maintain dependency chains. Dependency chains ensure that the resources a program requires to run are available. For instance, if a resource was monitoring a backup application that was backing up to Oracle ADVM volume, the backup application would want to ensure that it specified the Oracle ADVM volume resource in its `START` and `STOP` dependency list. Because the Oracle ADVM volume resource will enable the volume, this ensures that the volume is available before the backup begins.

- Oracle ACFS file systems are either manually mounted or dismounted using an Oracle ACFS or Oracle Clusterware command-line tool, or automatically mounted or dismounted based on an Oracle Clusterware resource action.

For example, a file system hosting an Oracle Database home is named in the dependency list of the associated Oracle Database resource such that issuing a start on the database resource results in mounting the dependent Oracle ACFS hosted database home file system.

Oracle ACFS file system resources provide the following actions:

- MOUNT

During the *START* operation the resource mounts the file system on the path configured in the resource. The Oracle ACFS file system resource requires all components of the Oracle ASM stack to be active (volume device, ASM) and ensures that they are active before attempting the mount.

- UNMOUNT

During the *STOP* operation, the resource attempts to unmount a file system.

- Oracle provides two resource types for Oracle Highly Available NFS. For more information, refer to [“High Availability Network File Storage for Oracle Grid Infrastructure”](#).

As with all Oracle Clusterware resources, these resources provide for high availability by monitoring the underlying device, file system, or driver to ensure that the object remains available. In the event that the underlying object becomes unavailable, each resource attempts to make the underlying object available again.

High Availability Actions

The following are the actions of the High Availability resources:

- Oracle ACFS resource

This resource attempts to unmount the file system. After the unmount has succeeded, the resource remounts the file system, making the file system available again. If processes are active on the file system during unmount, the resource identifies and terminates those processes.

- Oracle ADVN resource

This resource attempts to disable any volume device, and then reenables the volume device. At that point, any configured Oracle ACFS resource can remount the file system. If processes are active on the volume during this period, the resource identifies and terminates the processes.

Creating Oracle ACFS Resources

Oracle ACFS resources can be created with the following methods:

- Oracle ASM Configuration Assistant (ASMCA) provides a GUI that exposes the most common functionality. In all cases, creating a file system resource does not format the underlying file system. Attempts to start the resource require the user to format the file system either manually or with ASMCA.
- *SRVCTL* provides a highly flexible command line utility for creating Oracle ACFS file system resources through the *filesystem* object. Oracle ACFS resources

created through this mechanism have access to the full feature set, including server pools.

- `acfsutil` commands provide an alternative method to create Oracle ACFS file system resources using the *registry* object. Oracle ACFS resources created through this methodology have access to a limited set of options.

The differences between `SRVCTL` and `acfsutil` commands are:

- Oracle ACFS resources created through `SRVCTL` and specifying a server pool or list of nodes are only mounted on one of those nodes. (node-local)
- Oracle ACFS resources created through `SRVCTL` can take advantage of Oracle Server Pools.
- Oracle ACFS resources created through `acfsutil` commands and specifying a list of nodes are mounted on all listed nodes. (node-local)
- Oracle ACFS resources created through `acfsutil` commands are created with `AUTOSTART` set to `ALWAYS`.
- Oracle ACFS resources created through `SRVCTL` allow for advanced Application ID functionality. Using this functionality enables the resource type to be set by the administrator. After the type is set, other resources can depend on this type, allowing different node-local file systems to be used to fulfill dependencies on each node. In a simplified example, this would allow the administrator to have a different device mounted on the `/log` directory on each node of the cluster, and be able to run an Apache resource. The Apache resource would specify the new type in its resource dependency structure, rather than specifying an individual resource.
- Oracle ACFS resources created through `SRVCTL` can specify additional `AUTOSTART` parameters. These parameters can be used to prevent the resource from starting on stack startup, to always force the resource to start, or to only start the resource if it was previously running.
- Oracle ACFS resources created through `SRVCTL` have access to functionality such as accelerator volumes.

The common elements of both `SRVCTL` and `acfsutil` commands are:

- User

This is an additional user that can act upon the resource. By default, you must be the `root` user to start and stop an Oracle ACFS resource.
- Options

These are mount options that should be used to mount the file system when the resource is starting.

Node-Local or Clusterwide File Systems

When creating Oracle ACFS file system resources, you can create a node-local file system or to create a clusterwide file system.

- Node-local

This file system type is limited to the number of nodes it can mount on. Depending on if it is created with `SRVCTL` or `acfsutil` commands, it may only mount on one node, a subset of nodes, or all the configured nodes. In some cases, this could look the same as a full cluster configuration, but if new nodes are added to the

cluster, the file system is not automatically mounted on them without modifying the list of allowable nodes.

- **Clusterwide**

This type of file system mounts on all nodes of the cluster, with no exceptions. When new members are added to the cluster, the file system is automatically available on them. This type of resource is required for certain configurations, such as Oracle Database or Oracle HANFS.

Monitoring Oracle ACFS resources

Similar to all Oracle Clusterware resources, Oracle ACFS resources enables you to monitor the state of the system. You can do this monitoring with the following commands:

- **Using SRVCTL commands**

When the command `srvctl status filesystem` or `srvctl status volume` is run, the output of the command reports if the file system is mounted or the volume is enabled, and which nodes this is true on.

- **Using CRSCTL commands**

When the `crsctl status resource` command is run, a state of `ONLINE` is reported for each resource that is available, whether through a mounted file system or an enabled volume. A state of `OFFLINE` is reported for each resource that is not available, whether through an unmounted file system or a disabled volume. Additional status may be presented in the `STATUS` field of this output.

Stopping Oracle ACFS resources

You can be stop Oracle ACFS file system resources with the following methods:

- You can stop the entire Oracle Clusterware stack. When the Oracle Clusterware stack is stopped, all Oracle ACFS resources are automatically stopped.
- To stop individual resources, you can use SRVCTL management commands with the `filesystem` or `volume` object. The command may require the `-force` option if there are other resources that are depending on the resource that you are attempting to stop.
- You may engage a manual action, such as running `umount` on a file system or by manually stopping a volume using `ASMCMD` or `SQL*Plus` commands. In this case, the Oracle ACFS resource transitions to the `OFFLINE` state automatically.

Oracle ACFS resource Limitations

Oracle ACFS has the following resource limitations:

- All Oracle ACFS resources require `root` privileges to create.
- All Oracle ACFS resources require `root` privileges to remove.
- All Oracle ACFS file system resources require `root` privileges to act upon, such as starting and stopping the resources, but can be configured to allow another user, such as a database user, to do so. In this case, the `root` user must be used to configure the resource.
- All Oracle ADVM volume resources allow the `ASMADMIN` user to act upon them.

- All Oracle ACFS resources are only available in Oracle RAC mode. Oracle ACFS resources are not supported in Oracle Restart configurations. For more information about Oracle ACFS and Oracle Restart, refer to “[Oracle ACFS and Oracle Restart](#)”.

Oracle ACFS and Dismount or Shutdown Operations

It is important to dismount any active file system configured with an Oracle ADVM volume device file before an Oracle ASM instance is shutdown or a disk group is dismounted. After the file systems are dismounted, all open references to Oracle ASM files are removed and associated disk groups can be dismounted or the instance shut down.

If the Oracle ASM instance or disk group is forcibly shut down or fails while an associated Oracle ACFS is active, the file system is placed into an offline error state. If any file systems are currently mounted on Oracle ADVM volume files, the SHUTDOWN ABORT command should not be used to terminate the Oracle ASM instance without first dismounting those file systems. Otherwise, applications encounter I/O errors and Oracle ACFS user data and metadata being written at the time of the termination may not be flushed to storage before the Oracle ASM storage is fenced. If it is not possible to dismount the file system, then you should run two `sync (1)` commands to flush cached file system data and metadata to persistent storage before issuing the SHUTDOWN ABORT operation.

Any subsequent attempt to access an offline file system returns an error. Recovering a file system from that state requires dismounting and remounting the Oracle ACFS file system. Dismounting an active file system, even one that is offline, requires stopping all applications using the file system, including any shell references. For example, a previous change directory (`cd`) into a file system directory. The Linux `fuser` or `lsof` commands or Windows `handle` command list information about processes and open files.

For information about shutting down an Oracle ASM instance, see “[About Shutting Down an Oracle ASM Instance](#)”. For information about dismounting a disk group, see “[Mounting and Dismounting Disk Groups](#)”.

Oracle ACFS Security

Oracle ACFS security provides realm-based security for Oracle ACFS file systems, enabling you to create realms to specify security policies for users and groups to determine access on file system objects. This security feature provides a finer-grained access control on top of the access control provided by the operating system. Oracle ACFS security can use the encryption feature to protect the contents of realm-secured files stored in Oracle ACFS file systems.

Oracle ACFS security uses realms, rules, rule sets, and command rules to enforce security policies.

- An Oracle ACFS security realm is a group of files or directories that are secured for access by a user or a group of users. Realms are defined with rule sets which contain groups of rules that apply fine grain access control. Oracle ACFS security realms can also be used as containers to enable encryption.
- Oracle ACFS security rules are Boolean expressions that evaluate to true or false based on a system parameter on which the rule is based.
- Oracle ACFS rule sets are collection of rules. Rule sets evaluate to TRUE or FALSE based on the evaluation of the rules a rule set contains.

- Oracle ACFS command rules are associations of the file system operation to a rule set. For example, the association of a file system create, delete, or rename operation to a rule set. Command rules are associated with an Oracle ACFS realm.

An existing operating system user must be designated as the first Oracle ACFS security administrator and an existing operating system group must be designated as the security administrator *admin* group. Security administrators must be members of the designated security group. Additional users can be designated as security administrators. An Oracle ACFS security administrator can manage encryption for an Oracle ACFS file system on a per-realm basis. An Oracle ACFS security administrator is authenticated for security operations with a security realm password, not the operating system password of the user.

The first security administrator is created during the initialization of Oracle ACFS security with the `acfsutil sec init` command which is run by the root user. When the first security administrator is created, the administrator is assigned a password that can be changed by the administrator. Each time a security administrator runs an `acfsutil sec` command, the administrator is prompted for the security password. The security realm passwords for administrators are stored in a wallet created during the security initialization process. This wallet is located in the Oracle Cluster Registry (OCR).

Auditing and diagnostic data are logged for Oracle ACFS security. The log files include information such as `acfsutil` commands that have been run, the use of security or system administrator privileges, and run-time failures such as realm check authorization failures.

Auditing events, such as realm creation or encryption enabled, are written to these log files only if auditing is not enabled for on the file system. If auditing is enabled, these events are written into the audit trail. Diagnostic messages related to security and encryption are always written to the `sec-hostname_fsid.log` file regardless of whether auditing is enabled or not. For information about Oracle ACFS auditing, refer to [“Oracle ACFS Auditing”](#).

Logs are written to the following files:

- `mount_point/.Security/realm/logs/sec-hostname_fsid.log`

The directory is created with `acfsutil sec prepare` command and protected by Oracle ACFS security. Refer to [“acfsutil sec prepare”](#).

- `GRID_HOME/log/hostname/acfs/security/acfssec.log`

The messages that are logged to this file are for commands that are not associated with a specific file system, such as `acfsutil sec init`. The directory is created during installation and is owned by the root user.

When an active log file grows to a pre-defined maximum size (10 MB), the file is automatically moved to `log_file_name.bak`, the administrator is notified, and logging continues to the regular log file name. When the administrator is notified, the administrator must archive and remove the `log_file_name.bak` file. If an active log file grows to the maximum size and the `log_file_name.bak` file exists, logging stops until the backup file is removed. After the backup log file is removed, logging restarts automatically.

Oracle ACFS security protects the following objects from unauthorized accesses:

- Realm-secured directories and user files

The directories and files reside on a file system secured by Oracle ACFS security.

- The Oracle ACFS security directory (*mount_point/.Security*) and its contents
The security directory contains the log files in plain-text format and a security metadata backup file in XML format. The log files generated by Oracle ACFS security can only be accessed by valid Oracle ACFS security administrators.

- Oracle ACFS security objects

These objects are the security realms, rules, and rule sets used to manage Oracle ACFS security.

Access to files in a security realm of an Oracle ACFS file system must be authorized by both the security realm and the underlying operating system permissions, such as (owner, group, other) permissions on Linux and Access Control Lists (ACLs) on Windows. Each access to a realm-secured file is first checked for security realm authorization. If the access is authorized by the security realm, then access to the files is checked by the underlying operating system access control checks. If both checks pass, access is allowed to the realm-secured file.

Note the following when working with Oracle ACFS security:

- Oracle ACFS security does not provide any protection for data sent on the network.
- A copy of a realm-protected file is not realm-protected unless the copy is made in a security realm-protected directory.

Some applications, such as the `vi` editor, re-create a file when the file is modified. The modified file is saved as a temporary file, the original file is removed, and temporary file is copied with the original file name as the destination name. This process creates a new file. If the new file is created in a realm-protected directory, the security policies of the realm also apply to the new file. If the new file is not created in a realm-protected directory, then the new file is not realm-protected. If you are planning to copy a realm-protected file, you should ensure that the parent directory is also security realm protected.

Security policies also apply to any temporary files created in a realm-protected directory.

To use Oracle ACFS security functionality on Linux, the disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.2 or higher. To use Oracle ACFS security functionality on Windows, the disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.3 or higher. For information about disk group compatibility, refer to [“Disk Group Compatibility”](#).

For information about Oracle ACFS security and snapshots, refer to [“About Oracle ACFS Snapshots”](#).

Security information for Oracle ACFS file systems is displayed in the `V$ASM_ACFS_SECURITY_INFO` view. For information about `V$ASM_ACFS` views, refer to [Using Views to Display Oracle ACFS Information](#).

To configure security for Oracle ACFS file systems, you can use the `acfsutil sec` command-line functions described in [“Securing Oracle ACFS File Systems”](#) and [“Oracle ACFS Command-Line Tools for Security”](#). Also, you can use ASMCA described in [“Managing Security and Encryption for Oracle ACFS with ASMCA”](#).

See Also:

Your operating system-specific (OS) documentation for information about setting up OS users and OS groups

Oracle ACFS Encryption

Oracle ACFS encryption enables you to encrypt data stored on disk (data-at-rest). The encryption feature protects data in an Oracle ACFS file system in encrypted format to prevent unauthorized use of data in the case of data loss or theft. Both encrypted and non-encrypted files can exist in the same Oracle ACFS file system.

Some encryption functionality requires system administrator privileges. This functionality includes the commands for initiating, setting, and reconfiguring encryption.

System administrators and Oracle ACFS security administrators can initiate encryption operations. Also, unprivileged users can initiate encryption for files they own.

Oracle ACFS encryption provides two type of encryption keys:

- File Encryption Key

This is a key for a file and is used to encrypt the data in the file.

- Volume Encryption Key

This is a key for a file system and is used to encrypt the file encryption keys.

You must first create the encryption key store, then specify file system-level encryption parameters and identify the directories. No extra steps are required for a user to read encrypted files if the user has the appropriate privileges for accessing the file data.

Oracle ACFS encryption supports both Oracle Cluster Registry (OCR) and Oracle Key Vault as a key store. Both OCR and Oracle Key Vault can be used in the same cluster. However, a single file system uses either OCR or Oracle Key Vault as a key store, but not both. Oracle Key Vault is currently only available with file systems on Linux.

See Also:

Oracle Key Vault Administrator's Guide for information about Oracle Key Vault

If you are using OCR as a key store, you should back up the OCR after creating or updating an encryption key to ensure there is an OCR backup that contains all of the volume encryption keys (VEKs) for the file system.

Oracle ACFS encryption protects data stored on secondary storage against the threat of theft or direct access to the storage medium. Data is never written to secondary storage in plaintext. Even if physical storage is stolen, the data stored cannot be accessed without the encryption keys. The encryption keys are never stored in plaintext. The keys are either obfuscated, or encrypted using a user-supplied password.

An Oracle ACFS security administrator can manage encryption parameters on a per-realm basis. After a file is placed under realm security, file-level encryption operations are not allowed on that file. Even if the realm security allows the file owner or the root user to open the file, file-level encryption operations are blocked. Encryption of realm-protected files is managed entirely by the Oracle ACFS security administrator, who can enable and disable encryption for files at a security realm level.

After a directory has been added to a security realm, all files created in the directory inherit the realm-level encryption parameters, not the directory or file system-level parameters. When a file is removed from its last security realm, the file is encrypted or decrypted to match the file system-level encryption status. The file is not re-encrypted to match file system-level parameters if it has been encrypted with security realm parameters.

A system administrator cannot rekey realm-secured files at the file system or file level. To ensure all realm-secured files are encrypted with the most recent volume encryption key (VEK), you must first remove encryption from all realms, and then re-enable encryption. This action re-encrypts all files with the most recent VEK.

Auditing and diagnostic data are logged for Oracle ACFS encryption. The log files include information such as `acfsutil` commands that have been run, the use of security or system administrator privileges, and run-time failures. Logs are written to the following files:

- `mount_point/.Security/encryption/logs/encr-hostname_fsid.log`

The directory is created with `acfsutil encr set` command and protected by Oracle ACFS security if security is enabled. Refer to “[acfsutil encr set](#)”.

- `GRID_HOME/log/hostname/acfs/security/acfssec.log`

The messages that are logged to this file are for commands that are not associated with a specific file system, such as `acfsutil encr init`. The directory is created during installation and is owned by the root user.

When an active log file grows to a pre-defined maximum size (10 MB), the file is automatically moved to `log_file_name.bak`, the administrator is notified, and logging continues to the regular log file name. When the administrator is notified, the administrator must archive and remove the `log_file_name.bak` file. If an active log file grows to the maximum size and the `log_file_name.bak` file exists, logging stops until the backup file is removed. After the backup log file is removed, logging restarts automatically.

Note the following when working with Oracle ACFS encryption:

- A copy of an encrypted file is not encrypted unless the copy of the file is made in an encrypted directory.

Some applications, such as the `vi` editor, re-create a file when the file is modified. The modified file is saved as a temporary file, the original file is removed, and temporary file is copied with the original file name as the destination name. This process creates a new file. The new file is not encrypted unless it is created in an encrypted directory. If you are planning to copy an encrypted file, you should ensure that the parent directory is also encrypted.

- Using encryption with database files on Oracle ACFS is not supported.

To use Oracle ACFS encryption functionality on Linux, the disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.2 or higher. The disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.3 or higher on Linux for the following cases:

- If encryption is configured for the first time on Oracle ASM 11g Release 2 (11.2.0.3).
- If encryption parameters must be changed or a new volume encryption key must be created following a software upgrade to Oracle ASM 11g Release 2 (11.2.0.3). For information, see “[acfsutil encr set](#)” and “[acfsutil encr rekey](#)”.

To use Oracle ACFS encryption functionality on Windows, the disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.3 or higher.

For information about disk group compatibility, refer to [“Disk Group Compatibility”](#).

For information about Oracle ACFS encryption and snapshots, refer to [“About Oracle ACFS Snapshots”](#).

Encryption information for Oracle ACFS file systems is displayed in the `V$ASM_ACFS_ENCRYPTION_INFO` view. For information about `V$ASM_ACFS` views, refer to [Using Views to Display Oracle ACFS Information](#).

To configure encryption and manage encrypted Oracle ACFS file systems, you can use the `acfsutil encr` command-line functions described in [“Encrypting Oracle ACFS File Systems”](#) and [“Oracle ACFS Command-Line Tools for Encryption”](#). Also, you can use Oracle ASM Configuration Assistant with encryption features as described in [“Managing Security and Encryption for Oracle ACFS with ASMCA”](#).

Oracle ACFS Auditing

Oracle ACFS auditing provides auditing capabilities for Oracle ACFS security and encryption. This auditing framework produces a separate audit trail for each Oracle ACFS file system on each individual node, and enforces separation of duties regarding the management and review of this audit source.

Audit sources are the source of events, such as Oracle ACFS security and Oracle ACFS encryption. Audit trails are the logs where the audit records are written.

This section contains the following topics:

- [About Oracle ACFS Auditing](#)
- [Audit Trail File](#)
- [File Access Events](#)
- [Privilege Use Events](#)
- [Evaluation Result Events](#)

About Oracle ACFS Auditing

Both Oracle ACFS security and encryption are also audit sources, and these sources can be enabled and disabled by an Oracle ACFS audit manager. These sources generate events as a result of the execution of Oracle ACFS security or encryption commands.

The Oracle ACFS security administrator can enable auditing at the realm level so that security violations and authorizations can also be audited as well as enabling auditing on security to audit all the events executed by a security administrator. An Oracle ACFS security source must be enabled before Oracle ACFS realm security auditing can be used.

Setting the realm auditing policy to audit all authorizations and violations for all command rules can cause the audit trail to quickly increase to its maximum size. Administrators should carefully adjust the auditing level to their requirements and be aware that auditing policies generating more verbose auditing output require additional active monitoring and management, such as archiving and purging, of the audit trail and audit trail backup files.

Along with the generation of a file system audit source, Oracle ACFS auditing allows fine-grained auditing policies to be set separately on each realm basis. The Oracle ACFS auditing capability provides the infrastructure for an audit vault collector to import data into Oracle Audit Vault and Database Firewall. The collector is separate from Oracle ACFS and functions as means for Oracle ACFS auditing data to be imported into Audit Vault Server.

The responsibilities for configuration and management of the audit source are separated into the Oracle ACFS audit manager and Oracle ACFS auditor roles. The system administrator has the authority to add and remove users to and from the Oracle ACFS audit manager and Oracle ACFS auditor operating system (OS) groups.

The Oracle ACFS audit managers have access to the contents of audit sources and can read audit data; however, the audit managers cannot modify the audit sources. The set of Oracle ACFS audit managers is the same across a cluster.

The Oracle ACFS auditors are responsible for viewing and analyzing the contents of the audit source, such as indicating to the Oracle ACFS audit managers which records have been analyzed and archived and are safe to purge. The Oracle ACFS auditors should be the only users on the system with access to the contents of the audit source. The Oracle ACFS auditor do not have the required permissions to remove or purge audit records. The set of Oracle ACFS auditors is the same across a cluster.

The audit archiving process renames audit trail log files (.log) to a audit trail backup file (.log.bak) and generates an XML file, which can be imported by Audit Vault Server. Audit Vault Server has only read access to the audit trail directory and functions as an auditor in this case. After the data from the XML file is imported in the Audit Vault Server, the auditor function marks the audit trail backup file as read, and then audit manager can execute a purge to remove audit trail backup files and XML files.

To configure auditing for an Oracle ACFS file system, run the `acfsutil audit init` command to initialize auditing for Oracle ACFS and then run `acfsutil audit enable` to enable auditing for Oracle ACFS encryption or security on the specified file system. For information about the `acfsutil audit` commands, refer to [“Oracle ACFS Command-Line Tools for Auditing”](#).

For information about enabling or disabling auditing for specific commands in an Oracle ACFS security realm, refer to the `acfsutil sec realm audit enable` and `acfsutil sec realm audit disable` commands described in [“Oracle ACFS Command-Line Tools for Security”](#).

For information about views that are relevant to Oracle ACFS auditing, refer to [“Views Containing Oracle ACFS Information”](#).

See Also:

- *Oracle Audit Vault and Database Firewall Administrator’s Guide* for information about the Audit Vault Server
 - Your operating system-specific (OS) documentation for information about setting up OS users and OS groups
-

Audit Trail File

Audit trail files consist of a set of audit records. Each audit record represents a single event. Audit trail files are located in the `mount_point/.Security/audit` directory.

Audit trail files generated by Oracle ACFS auditing are meant to be available for the following:

- Manual review by an Oracle ACFS auditor using text viewing tools
- Import into Oracle Audit Vault and Database Firewall
- Third party products that can parse and import the audit sources

The audit trail file consists of audit records. There are several different types of audit records, each of which represent a unique type of event and contain different information relevant to diagnosing the event. The types of events are:

- [File Access Events](#)
- [Privilege Use Events](#)
- [Evaluation Result Events](#)

The combination of audit record fields entered in the audit trail file depends on the event type.

Each record is written to the audit trail file as a set of field names and values. Depending on the type of record, the number and type of fields may vary. Fields consist of a name and value pair, in the form `field name:value`, followed by an end of line character.

The audit record fields that can be present in the audit trail file are described in the following list. The string in parenthesis is the field name that appears in the audit trail log file.

- **Timestamp (Timestamp):** The time at which the event occurred, always specified in UTC. The format for the time stamp is: `MM/DD/YYYY HH:MM:SS UTC`
- **Event Code (Event):** A code identifying the type of event. For the list of evaluation result codes, refer to "[File Access Events](#)" and "[Privilege Use Events](#)".
- **Source (Source):** `Oracle ACFS`
- **User identification (User):** The user who triggered the event. On Linux platforms this is a user ID and on Windows this is the user SID.
- **Group identification (Group):** The primary group of the user who triggered the event. On Linux platforms this is the ID the primary group of the user and on Windows this is the SID of the primary group of the user.
- **Process identification (Process):** The current process ID.
- **Host name (Host):** The host which recorded the event.
- **Application name (Application):** The application name for the current process.
- **Realm name (Realm):** The name of the realm which was violated, or the realm that is authorized and is protecting the file.

- File name (File): The file name which the user was accessing.
- Evaluation Result (Evaluation Result): This field contains the information about the result of the command executed. For the list of evaluation result codes, refer to “[Evaluation Result Events](#)”.
- File system Id (FileSystem-ID):
- Message (Message): The message field has the information about the command executed and its result.

[Example 1](#) shows an example of an audit trail file.

Example 1 Sample audit trail file

```

Timestamp: 06/08/12 11:00:37:616 UTC
Event: ACFS_AUDIT_READ_OP
Source: Oracle_ACFS
User: 0
Group: 0
Process: 1234
Host: slc01hug
Application: cat
Realm: MedicalDataRealm
File: f2.txt
Evaluation Result: ACFS_AUDIT_REALM_VIOLATION
FileSystem-ID: 1079529531
Message: Realm authorization failed for file ops READ

Timestamp: 06/08/12 11:00:37:616 UTC
Event: ACFS_AUDIT_WRITE_OP
Source: Oracle_ACFS
User: 102
Group: 102
Process: 4567
Host: slc01hug
Application: vi
Realm: PayrollRealm,SecuredFiles
File: f2.txt
Evaluation Result: ACFS_AUDIT_REALM_AUTH
FileSystem-ID: 1079529531
Message: Realm authorization succeeded for file ops WRITE

Timestamp: 06/08/12 10:42:20:977 UTC
Event: ACFS_SEC_PREPARE
Source: Oracle_ACFS
User: 507867
Group: 8500
Process: 603
Host: slc01hug
Application: acfsutil.bin
Evaluation Result: ACFS_CMD_SUCCESS
FileSystem-ID: 1079529531
Message: acfsutil sec prepare: ACFS-10627: Mount point '/mnt' is now
prepared for security operations.

```

File Access Events

File access events include both realm authorization and violation records. These events share a similar structure with all events, but have a different event code. The Evaluation Result (Evaluation Result) field can contain either ACFS_AUDIT_REALM_VIOLATION or ACFS_AUDIT_REALM_AUTH.

The possible event code (Event) for file access events include the following:

- ACFS_AUDIT_APPENDFILE_OP

- ACFS_AUDIT_CHGRP_OP
- ACFS_AUDIT_CHMOD_OP
- ACFS_AUDIT_CHOWN_OP
- ACFS_AUDIT_CREATEFILE_OP
- ACFS_AUDIT_DELETEFILE_OP
- ACFS_AUDIT_EXTEND_OP
- ACFS_AUDIT_GET_EXTATTR_OP
- ACFS_AUDIT_LINKFILE_OP
- ACFS_AUDIT_MKDIR_OP
- ACFS_AUDIT_MMAPREAD_OP
- ACFS_AUDIT_MMAPWRITE_OP
- ACFS_AUDIT_MUTABLE_OP
- ACFS_AUDIT_OPENFILE_OP
- ACFS_AUDIT_OVERWRITE_OP
- ACFS_AUDIT_READ_OP
- ACFS_AUDIT_READDIR_OP
- ACFS_AUDIT_RENAME_OP
- ACFS_AUDIT_RMDIR_OP
- ACFS_AUDIT_SET_EXTATTR_OP
- ACFS_AUDIT_SYMLINK_OP
- ACFS_AUDIT_TRUNCATE_OP
- ACFS_AUDIT_WRITE_OP

Privilege Use Events

Privilege use events include security commands run by the security administrator or system administrator, and encryption commands run by the system administrator or file owners.

The ACFS_AUDIT_INIT, ACFS_SEC_INIT, and ACFS_ENCR_INIT events are written into the global log that is located in Oracle Grid Infrastructure home.

The possible event code (Event) for privilege use events include the following:

- ACFS_AUDIT_ARCHIVE
- ACFS_AUDIT_DISABLE
- ACFS_AUDIT_ENABLE
- ACFS_AUDIT_INIT

- ACFS_AUDIT_PURGE
- ACFS_AUDIT_READ
- ACFS_ENCR_FILE_OFF
- ACFS_ENCR_FILE_ON
- ACFS_ENCR_FILE_REKEY
- ACFS_ENCR_FS_OFF
- ACFS_ENCR_FS_ON
- ACFS_ENCR_INIT
- ACFS_ENCR_SET
- ACFS_ENCR_SET_UNDO
- ACFS_ENCR_VOL_REKEY
- ACFS_ENCR_WALLET_STORE
- ACFS_REALM_AUDIT_DISABLE
- ACFS_REALM_EDIT_ENCR
- ACFS_REALM_AUDIT_ENABLE
- ACFS_SEC_LOAD
- ACFS_SEC_PREPARE
- ACFS_SEC_PREPARE_UNDO
- ACFS_SEC_REALM_ADD
- ACFS_SEC_REALM_CLONE
- ACFS_SEC_REALM_CREATE
- ACFS_SEC_REALM_DELETE
- ACFS_SEC_REALM_DESTROY
- ACFS_SEC_RULE_CREATE
- ACFS_SEC_RULE_DESTROY
- ACFS_SEC_RULE_EDIT
- ACFS_SEC_RULESET_CREATE
- ACFS_SEC_RULESET_DESTROY
- ACFS_SEC_RULESET_EDIT
- ACFS_SEC_SAVE

Evaluation Result Events

Evaluation result event codes provide information about the execution status of a command.

The evaluation result event codes can be one of the following:

- `ACFS_AUDIT_REALM_VIOLATION` – The user executing the command does not have the proper realm access permission to execute the command.
- `ACFS_AUDIT_REALM_AUTH` - Indicates the result of a realm evaluation.
- `ACFS_AUDIT_MGR_PRIV` – Audit manager privileges are required, but have not been granted to the user.
- `ACFS_AUDITOR_PRIV` – Auditor privileges are required, but have not been granted to the user.
- `ACFS_CMD_SUCCESS` - The command has been successful in performing the task.
- `ACFS_CMD_FAILURE` - The command has failed in performing the task.
- `ACFS_ENCR_WALLET_AUTH_FAIL` – A system administrator provides an incorrect password when opening an encryption wallet.
- `ACFS_INSUFFICIENT_PRIV` – Either file owner or system administrator privileges are required, but have not been granted to the user.
- `ACFS_SEC_ADMIN_PRIV` – Security administrator privileges are required, but the user is not a security administrator
- `ACFS_SEC_ADMIN_AUTH_FAIL` – A valid security administrator fails to authenticate properly using their Oracle ACFS security administration password
- `ACFS_SYS_ADMIN_PRIV` – System administrator privileges are required, but have not been granted to the user.

Oracle ACFS Replication

Oracle ACFS replication enables replication of Oracle ACFS file systems across the network to a remote site, providing disaster recovery capability for the file system.

Note:

- Oracle ACFS replication functionality supports only one standby file system for each primary file system.
 - Oracle ACFS replication supports eight or fewer nodes mounting the primary file system.
 - The sites hosting the primary and standby file systems must be running the same operating system and must have the same system architecture.
 - The primary and standby sites should be running the same version of the Oracle Grid Infrastructure software. When upgrading the sites, update the standby site first.
 - The primary file system requires internal metadata files that are not visible to user-level commands, such as `du` or `ls`. The amount of internal storage for the primary file system is approximately 1 GB for each node. This extra internal storage accounts for the difference in storage usage between primary and standby file systems containing the same user files.
 - Oracle wallets should be used to manage security credentials when configuring the primary and standby file systems.
 - Using replication with database files on Oracle ACFS is not supported.
 - Oracle ACFS replication is not supported with Oracle Restart.
-
-

The source Oracle ACFS file system of an Oracle ACFS replication is referred to as a primary file system. The target Oracle ACFS file system of an Oracle ACFS replication is referred to as a standby file system.

A site can host both primary and standby file systems. For example, if there are cluster sites A and B, a primary file system hosted at site A can be replicated to a standby file system at site B. Also, a primary file system hosted at site B can be replicated to a standby file system at site A. However, an Oracle ACFS file system cannot be used as a primary and a standby file system.

Oracle ACFS replication captures file system changes written to disk for a primary file system and records the changes in files called replication logs. These logs are transported to the site hosting the associated standby file system where background processes read the logs and apply the changes recorded in the logs to the standby file system. After the changes recorded in a replication log have been successfully applied to the standby file system, the replication log is deleted from the sites hosting the primary and standby file systems.

It is critical that there is enough disk space available on both sites hosting the primary and the standby file systems to contain the replication logs. If the primary file system runs out of space, applications running on the file system may fail because Oracle ACFS cannot create a new replication log to capture the file system changes made by the application. If the standby file system runs out of space, it cannot accept new replication logs from the primary file system and cannot apply those changes to the standby file system. In addition, replication logs accumulate on the primary file system and consume the available disk space.

If the primary file system has less than 2 GB available free disk space, Oracle ACFS attempts to automatically terminate replication on the primary file system. This action

prevents further consumption of disk space for replication operations and frees disk space consumed by any replication logs that remain. The auto-terminate process can prevent the primary file system from running out of space in most cases, but it is still possible that the auto-terminate process does not occur quickly enough. Before reaching the 2 GB limit, Oracle ACFS writes warnings about the free space problem in the Oracle Grid Infrastructure home alert log.

You should prevent both the primary file system and the standby file system from running out of space. If either file system runs out of available storage, you should either expand the file system or remove files from the file system to free up space. If the primary file system runs out of space and you decide to free up space by removing files, you should only remove files that are not being replicated because the removal of a file that is replicated is captured in a replication log. Another option is to delete any Oracle ACFS snapshots. For information about resizing an Oracle ACFS file system, refer to [“acfsutil size”](#).

Because replication logs can accumulate when replication is paused, you should resume replication soon after pausing replication. For information on pausing and resuming replication, refer to [“acfsutil repl pause”](#) and [“acfsutil repl resume”](#).

Before using replication on a file system, ensure that you have checked the following:

- There is sufficient network bandwidth to support replication between the primary and standby file systems.
- The configuration of the sites hosting the primary and standby file systems allow the standby file system to keep up with the rate of change on the primary file system.
- The standby file system has sufficient capacity to manage the replication logs that are sent.
- There is sufficient storage capacity to hold excess replication logs that might collect on the primary and the standby file systems when the standby file system cannot process replication logs quickly. For example, this situation can occur during network problems or maintenance on the site hosting the standby file system.
- The primary file system must have a minimum size of 4 GB for each node that is mounting the file system. The standby file system must have a minimum size of 4 GB and should be sized appropriately for the amount of data being replicated and the space necessary for the replication logs sent from the primary file system.

See Also:

For information about tuning the network, refer to the documentation at the MAA link on Oracle Technology Network:

<http://www.oracle.com/technetwork/database/features/availability/maa-096107.html>

Relevant information on tuning the network can be found in the *Data Guard Redo Transport & Network Configuration* paper.

Directories and files in an Oracle ACFS file system can be tagged to select the objects that you want to replicate in a file system. For information on tagging, see [“Oracle ACFS Tagging”](#).

Before replicating an Oracle ACFS file system, a replication configuration must be established that identifies information such as the site hosting the primary file system, the site hosting the standby file system, the file system to be replicated, mount point of the file system, and a list of tags if desired.

The primary and standby sites must share the same user and group configurations, including all `uids` and `gids` in use in the file system. Because the replication daemons run with the credentials of `oinstall` and the Oracle ASM administration group, the permissions on the mount points must be configured so that the daemons are able to read and traverse the directory mount point in order to access and create files under the `.ACFS/repl` directory, which is the internal working location for replication logs and associated files.

To use Oracle ACFS replication functionality on Linux, the disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.2 or higher for the disk groups that contain the primary and standby file systems. To use Oracle ACFS replication functionality on Windows, the disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.3 or higher. To use Oracle ACFS replication functionality on Solaris or AIX, the disk group compatibility attributes for ASM and ADVM must be set to 12.1 or higher. For information about disk group compatibility, refer to “[Disk Group Compatibility](#)”.

To use Oracle ACFS replication on Solaris Sparc hardware, the system must be running Solaris 10 update 8 or later.

To configure replication and manage replicated Oracle ACFS file systems, use the `acfsutil repl` command-line functions described in “[Replicating Oracle ACFS File Systems](#)” and “[Oracle ACFS Command-Line Tools for Replication](#)”.

Oracle ACFS Tagging

Oracle ACFS tagging assigns a common naming attribute to a group of files. Oracle ACFS Replication can use this tag to select files with a unique tag name for replication to a different remote cluster site. The tagging option avoids having to replicate an entire Oracle ACFS file system.

Oracle ACFS implements tagging with Extended Attributes. Some editing tools and backup utilities do not retain the Extended Attributes of the original file by default; you must set a specific switch. The following list describes the necessary requirements and switch settings for some common utilities to ensure Oracle ACFS tag names are preserved on the original file.

- The `cp` command requires flags to preserve tag names.

Install the `coreutils` library (version `coreutils-5.97-23.el5_4.1.src.rpm` or `coreutils-5.97-23.el5_4.2.x86_64.rpm` or later) on Linux to install versions of the `cp` command that supports Extended Attribute preservation with the `--preserve=xattr` switch and the `mv` command that supports Extended Attribute preservation without any switches.

`cp` does not preserve tag names assigned to symbolic link files.

The `cp` switches required to preserve tag names on files and directories are:

- Linux: `--preserve=xattr`
- Solaris: `-@`
- AIX: `-U`

- Windows: no switch necessary
- The `cpio` file transfer utility requires flags to preserve tag names.
The `cpio` switches required to preserve tag names on files and directories are:
 - Linux: `cpio` does not preserve tag names
 - Solaris: `-@` is required to preserve or restore tag names for files and directories, but does not preserve tag names for symbolic link files
 - AIX: `-U` is required to preserve or restore tag names for files and directories, but does not preserve tag names for symbolic link files
 - Windows: not available
- `emacs` requires that the `backup-by-copying` option is set to a non-nil value to preserve tag names on the original file name rather than a backup copy. This option must be added to the `.emacs` file.
- The `pax` file transfer utility requires flags to preserve tag names.
The `pax` switches required to preserve tag names on files and directories are:
 - Linux: `pax` does not preserve tag names
 - Solaris: `-@` is required to preserve or restore tag names for files and directories, but does not preserve tag names for symbolic link files
 - AIX: `-U` is required to preserve or restore tag names for files and directories, but does not preserve tag names for symbolic link files
 - Windows: not available
- The `rsync` file transfer utility requires flags to preserve tag names.
The `rsync` switches required to preserve tag names on files and directories are:
 - Linux: `-X -l` are required to preserve tag names for files and directories, but these switches do not preserve tag names for symbolic link files
 - Solaris: `rsync` does not preserve tag names
 - AIX: not available
 - Windows: not available
- The `tar` backup utility can have flags set on the command line to preserve tag names on a file. However, `tar` does not retain the tag names assigned to symbolic link files.
The `tar` backup utility on Windows currently provides no support to retain tag names as no switch exists to save Extended Attributes.
The `tar` switches required to preserve tag names on files and directories are:
 - Linux: `--xattrs`
 - Solaris: `-@`
 - AIX: `-U`

- Windows: `tar` does not preserve tag names
- The `vim` or `vi` editors require the `set bkc=yes` option in the `.vimrc` (Linux) or `_vimrc` (Windows) file to make a backup copy of a file and overwrite the original. This preserves tag names on the original file.

To use Oracle ACFS tagging functionality on Linux, the disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.2 or higher. To use Oracle ACFS tagging functionality on Windows, the disk group compatibility attributes for ASM and ADVM must be set to 11.2.0.3 or higher. To use Oracle ACFS tagging functionality on Solaris or AIX, the disk group compatibility attributes for ASM and ADVM must be set to 12.1 or higher. For information about disk group compatibility, refer to [“Disk Group Compatibility”](#).

To configure tagging and manage tagged Oracle ACFS file systems, use the `acfsutil tag` command-line functions described in [“Tagging Oracle ACFS File Systems”](#) and [“Oracle ACFS Command-Line Tools for Tagging”](#). For information about Oracle ACFS tagging application programming interfaces (APIs), refer to [“Oracle ACFS Tagging Generic Application Programming Interface”](#).

Using Replication with Auditing, Encryption, and Security

Audited, encrypted, or security realm-secured file systems can be enabled on an Oracle ACFS file system on which replication has been configured. The replicated standby file system is secured with the same auditing, security, or encryption policies as the primary file system. For this replicated environment, the primary and standby file systems must both be 12.1 or higher installations. For more information about Oracle ACFS replication, refer to [“Oracle ACFS Replication”](#).

To ensure successful replication, the standby file system must be a generic file system without auditing, encryption, or security metadata on it. Oracle ACFS does not support using a standby file system that once had security or encryption and then had security or encryption removed. Additional conditions that must be met for Oracle ACFS auditing, encryption, and security are listed in this section.

Note the following about Oracle ACFS audited file systems:

- Before replicating an audit-enabled file system or auditing a replicated file system, auditing must be initialized on the standby file system.
- Auditing policies present on the primary file system are replicated to the standby and any policy actions taken on the primary file system are enacted on the standby file system.
- Two sets of audit trails are present on the standby file system. Trails from primary file system are replicated to the standby file system as ordinary files. File system activity may generate events on the standby file system, which are recorded in the audit trail for the standby file system. Audit trail names help distinguish the two sets of trails because they contain both the host name and FSID.

Note the following about Oracle ACFS encrypted file systems:

- Encrypted files on the primary file system remain encrypted on the standby file system with the same key and encryption parameters (algorithm and key length).
- Encryption operations done on the primary file system are replayed on the standby file system - on, off, and rekey.

- Encryption may be enabled before or after a file system is replicated. In either case, an encryption wallet is transparently created on the standby file system if one does not exist because `acfsutil encr init` has not been run on the standby file system.
- A password-protected wallet is not supported on the standby file system. If a PKCS wallet already exists on a site that is to be used as a standby file system, the administrator must use the `acfsutil keystore migrate` command to transfer all keys to an SSO wallet.

Note the following about Oracle ACFS secured file systems:

- Standby file systems should be initialized for security before replicating a security enabled file system.
- The rules, rule sets and realms are replicated to the standby file system and same policies exist on the standby file system. In terms of the policies and protection of files, the standby file system is exactly same.
- Replication can be enabled on a security enabled file system or security can be enabled on a replicated file system. As part of security preparation, security is also enabled on the standby file system.
- Having security and replication together on a file system does not require any extra user intervention or additional steps.
- A different set of security administrators or security administrator groups can be set up on the standby file system.

Oracle ACFS Plugins

The Oracle ACFS plugin functionality enables a user space application to collect *just-in-time* Oracle ACFS file and Oracle ADVM volume metrics from the operating system environment. Applications can use the Oracle ACFS plug-in infrastructure to create customized solutions that extend the general application file metric interfaces to include detailed Oracle ACFS file system and volume data.

The Oracle ACFS plug-in functionality can be enabled on separate Oracle ACFS file systems mounted on a standalone host or on one or more nodes of an Oracle Grid cluster where the Oracle ACFS file system is mounted. This functionality enables message communication between a node-local plugin enabled Oracle ACFS file system and an associated user space application module using Oracle ACFS plug-in application programming interfaces (APIs).

The plugin message APIs support both polling and posting message delivery models and multiple message payload types.

For information about Oracle ACFS plugin commands, refer to [“Oracle ACFS Command-Line Utilities”](#). For information about the Oracle ACFS plug-in application programming interface, refer to [“Oracle ACFS Plug-in Generic Application Programming Interface”](#).

High Availability Network File Storage for Oracle Grid Infrastructure

High Availability Network File Storage (NFS) for Oracle Grid Infrastructure provides uninterrupted service of NFS V2/V3/V4 exported paths by exposing NFS exports on Highly Available Virtual IPs (HAVIP) and using Oracle Clusterware agents to ensure that the HAVIPs and NFS exports are always online. While base NFS supports file locking, HANFS does not support NFS file locking.

Note:

- This functionality relies on a working NFS server configuration available on the host computer. You must configure the NFS server before attempting to use the Oracle ACFS NFS export functionality.
- This functionality is not available on Windows.
- This functionality is not supported in Oracle Restart configurations.
- The HAVIP cannot be started until at least one file system export resource has been created for it.

To set up High Availability NFS for Oracle Grid Infrastructure, perform the following steps:

1. Add and register a new HAVIP resource.

For example:

```
# srvctl add havip -id hrexports -address my_havip_name
```

In the example, *my_havip_name* is mapped in the domain name server (DNS) to the VIP address and is used by the client systems when mounting the file system.

The initial processing of `srvctl add havip` ensures that:

- The address being used is static, not dynamic
- Any DNS names resolve to only one host, not round-robin multiple DNS resolutions
- The network resource and provided IP address and resolved name are in the same subnet
- The name is not in use

SRVCTL creates the appropriate HAVIP name using the *id*, ensuring it is unique. As a final validation step, SRVCTL ensures that the *network* resource (if provided) of `ora.net#.network` exists. After this step, SRVCTL adds a new havip of type `ora.havip.type` with the name of `ora.id.havip`. In this example, the name is `ora.hrexports.havip`.

Next SRVCTL modifies HAVIP start dependencies, such as *active dispersion*; sets the stop dependencies; and ensures the *description* attribute (if provided) is appropriately set.

2. Create a shared Oracle ACFS file system.

High Availability NFS for Oracle Grid Infrastructure operates only with Oracle ACFS file systems configured for clusterwide accessibility and does not support Oracle ACFS file systems configured for access on particular subsets of cluster nodes. High Availability NFS is not supported with non-Oracle ACFS file systems.

For information on creating an Oracle ACFS file system, refer to [“Creating an Oracle ACFS File System”](#).

3. Register the Oracle ACFS file system.

For example:

```
$ srvctl add filesystem -device /dev/asm/d1volume1-295 -volume VOLUME1 \  
-diskgroup HR_DATA -mountpath /oracle/cluster1/acfs1
```

See Also:

Oracle Real Application Clusters Administration and Deployment Guide for information about the `srvctl add filesystem` command

4. Create an Oracle ACFS file system export resource.

For example:

```
# srvctl add exportfs -id hreexports -path /oracle/cluster1/acfs1 \  
-name hreexport1
```

After the file system export resource has been created, then you can start the HAVIP created in step 1 to export the file system using the `srvctl start havip` command.

The NFS mount option FSID is added to any export options, in the range of one billion or higher to minimize potential collisions with other FSIDs that are set on the server. This FSID option provides for reliable fail over between nodes and allows the usage of snapshot mounting.

The default mount and export options for configured exports are the defaults for the NFS server.

Relative paths that are fully-qualified are converted to absolute paths. Relative paths that are not fully-qualified are not accepted as an export path.

HAVIPs attempts to find the best server to run on based on available file systems and other running HAVIPs, but this dispersion only occurs during CSS membership change events, such as a node joining or leaving the cluster.

Note:

It is not recommended to start and stop exports individually; this functionality should be provided through the start and stop operations of HAVIP.

When HAVIP is not running, exports can exist on different nodes. After the associated HAVIP is started, the exports gather on a single node.

Clients that are using an export that is stopped while HAVIP is running raise the NFS error `estale`, and must dismount and remount the file system.

See Also:

- *Oracle Real Application Clusters Administration and Deployment Guide* for information about SRVCTL commands
 - *Oracle Clusterware Administration and Deployment Guide* for information about Oracle Clusterware resources
-
-

Overview of Oracle ASM Dynamic Volume Manager

Oracle ASM Dynamic Volume Manager (Oracle ADVM) provides volume management services and a standard disk device driver interface to clients. File systems and other disk-based applications send I/O requests to Oracle ADVM volume devices as they would to other storage devices on a vendor operating system.

An Oracle ADVM volume device is constructed from an Oracle ASM dynamic volume. One or more Oracle ADVM volume devices may be configured within each Oracle ASM disk group. The Oracle ADVM Driver maps I/O requests against an Oracle ADVM volume device to blocks in a corresponding Oracle ASM dynamic volume and disk set located within an Oracle ASM disk group. An Oracle ADVM volume device exports Oracle ASM volume manager features and ensures that volume mirrors remain consistent in the face of abnormal system shutdowns, Oracle ASM instance failures, or system failures.

Oracle ADVM extends Oracle ASM by providing a disk driver interface to Oracle ASM storage allocated as Oracle ADVM volume files. You can use Oracle ADVM to create virtual disks that contain file systems. These file systems contained on Oracle ADVM volumes are able to support files beyond Oracle Database files, such as executable files, report files, trace files, alert logs, and other application data files. Because Oracle ADVM volumes are actually Oracle ASM files, they require the same administrative privileges as the Oracle ASM files.

Oracle Automatic Storage Management Cluster File System (Oracle ACFS) communicates with Oracle ASM through the Oracle ADVM interface. With the addition of the Oracle ADVM, Oracle ASM becomes a complete storage solution of user data for both database and non-database file needs.

To add a volume to an Oracle ASM disk group, disk group attributes `COMPATIBLE.ASM` and `COMPATIBLE.ADVM` must be set to `'11.2'`.

Note:

Dynamic volumes supersede traditional device partitioning. Each volume is individually named and may be configured for a single file system. Oracle ADVM volumes may be created on demand from Oracle ASM disk group storage and dynamically resized as required. These attributes make Oracle ADVM volumes far more flexible than physical devices and associated partitioning schemes.

The Oracle ADVM functionality includes the following:

- The `ALTER DISKGROUP ADD | RESIZE | DROP | ENABLE | DISABLE | MODIFY VOLUME` SQL statements that manage Oracle ADVM volumes.

See [“Managing Oracle ADVM Volumes in a Disk Group”](#).

See Also:

Oracle Database SQL Language Reference for information about the `ALTER DISKGROUP` SQL statement

- ASMCMD command-line tools for managing Oracle ADVM volumes.

See [Managing Oracle ADVN with ASMCMD](#) .

- There are new V\$ASM views display information about Oracle ADVN volumes.

See [Using Views to Display Oracle ACFS Information](#) .

- Oracle ACFS operating system utilities for managing file systems and volume device files.

See [Managing Oracle ACFS with Command-Line Tools](#).

Using Views to Display Oracle ACFS Information

This chapter contains information about using dynamic views to display Oracle Automatic Storage Management Cluster File System (Oracle ACFS) and Oracle ASM Dynamic Volume Manager (Oracle ADVM) information.

- [Views Containing Oracle ACFS Information](#)
- [Oracle ACFS Support for Oracle Database File Mapping Views](#)

See Also:

Oracle Database Reference for information about all of the V\$ASM* dynamic performance views

Views Containing Oracle ACFS Information

You can use the views in [Table 1](#) to obtain information about Oracle Automatic Storage Management Cluster File System (Oracle ACFS). These views are accessible from the Oracle ASM instance.

Note:

- To display information about Oracle ACFS file systems or volumes that are located on nodes in an Oracle Flex ASM configuration, you must connect to the Oracle ASM proxy instance instead of the local Oracle ASM instance. For information about Oracle Flex ASM, refer to “[Managing Oracle Flex ASM](#)”.
 - When viewing space usage values in Oracle ACFS views on Windows systems, the values may differ from sizes in Windows folders. The mechanism used by **Folder Properties** on Windows systems only accounts for files and should be considered an approximate value.
-

Table 1 Oracle ASM dynamic views for Oracle ACFS information

View	Description
V\$ASM_ACFS_ENCRYPTION_INFO	Contains encryption information for each Oracle ACFS file system.
V\$ASM_ACFS_SECURITY_INFO	Contains security realm information for each Oracle ACFS file system.
V\$ASM_ACFS_SEC_ADMIN	Contains information about Oracle ACFS security administrator in the cluster.

View	Description
V\$ASM_ACFS_SEC_CMDRULE	Contains information about Oracle ACFS security command rules for each Oracle ACFS file system.
V\$ASM_ACFS_SEC_REALM	Contains information about every realm in the Oracle ACFS security realm for each Oracle ACFS file system.
V\$ASM_ACFS_SEC_REALM_FILTER	Contains information about every filter in the Oracle ACFS security realm for each Oracle ACFS file system. A filter is defined as a <code>commandrule/ruleset</code> pair in a realm.
V\$ASM_ACFS_SEC_REALM_GROUP	Contains information about every group in the Oracle ACFS security realm for each Oracle ACFS file system.
V\$ASM_ACFS_SEC_REALM_USER	Contains information about every user in the Oracle ACFS security realm for each Oracle ACFS file system.
V\$ASM_ACFS_SEC_RULE	Contains information about every Oracle ACFS security rule for each Oracle ACFS file system.
V\$ASM_ACFS_SEC_RULESET	Contains information about every Oracle ACFS security ruleset for each Oracle ACFS file system.
V\$ASM_ACFS_SEC_RULESET_RULE	Contains information about every rule in Oracle ACFS security ruleset for each Oracle ACFS file system.
V\$ASM_ACFSSNAPSHOTS	Contains snapshot information about every mounted Oracle ACFS file system.
V\$ASM_ACFSTAG	Contains all tag name information about files on all mounted Oracle ACFS file systems.
V\$ASM_ACFSVOLUMES	Contains information about mounted Oracle ADVM volumes, correlated with V\$ASM_FILESYSTEM.
V\$ASM_AUDIT_CLEAN_EVENTS	Contains information about the history of audit trail cleanup or purge events in an Oracle ASM instance.
V\$ASM_AUDIT_CLEANUP_JOBS	Contains information about the configured audit trail purge jobs in an Oracle ASM instance.
V\$ASM_AUDIT_CONFIG_PARAMS	Contains information about the currently configured audit trail properties in an Oracle ASM instance that are used by the <code>DBMS_AUDIT_MGMT PL/SQL</code> package.
V\$ASM_AUDIT_LAST_ARCH_TS	Contains information about the last archive timestamps set for audit trail cleanup or purges in an Oracle ASM instance.
V\$ASM_FILESYSTEM	Contains information about every mounted Oracle ACFS file system.
V\$ASM_VOLUME	Contains information about each Oracle ADVM volume that is a member of an Oracle ASM instance.
V\$ASM_VOLUME_STAT	Contains information about statistics for each Oracle ADVM volume.

Example 1 shows information displayed from the `V$ASM_ACFS_ENCRYPTION_INFO` view. The `FS_NAME` column contains the mount point. The `VOL_DEVICE` contains the name of the Oracle ADVM device.

See Also:

Oracle Database Reference for information about the `V$ASM_ACFS_ENCRYPTION_INFO` view

[Example 2](#) shows information displayed from the V\$ASM_ACFS_SECURITY_INFO view. The FS_NAME column contains the mount point. The VOL_DEVICE contains the name of the Oracle ADVM device.

See Also:

Oracle Database Reference for information about the V\$ASM_ACFS_SECURITY_INFO view

[Example 3](#) shows information displayed from the V\$ASM_ACFS_SEC_RULE view. The FS_NAME column contains the mount point.

[Example 4](#) shows information displayed from the V\$ASM_ACFS_SEC_RULESET view. The FS_NAME column contains the mount point.

[Example 5](#) shows information displayed from the V\$ASM_ACFS_SEC_RULESET_RULE view. The FS_NAME column contains the mount point.

[Example 6](#) shows information displayed from the V\$ASM_ACFSSNAPSHOTS view. The FS_NAME column contains the mount point. The VOL_DEVICE contains the name of the Oracle ADVM device.

See Also:

Oracle Database Reference for information about the V\$ASM_ACFSSNAPSHOTS view

[Example 7](#) shows information displayed from the V\$ASM_ACFSVOLUMES view. The PRIMARY_VOL column contains TRUE if the volume is the primary volume for the file system.

See Also:

Oracle Database Reference for information about the V\$ASM_ACFSVOLUMES view

[Example 8](#) shows information displayed from the V\$ASM_FILESYSTEM view.

The STATE column contains the status of the file system, either AVAILABLE or OFFLINE. An offline file system can only be dismounted; other attempts at access result in errors. Offline means that either the Oracle ASM instance is down, the disk group has been forced dismounted, or less commonly, a metadata I/O failure occurred or serious metadata corruption was detected. With a metadata I/O failure, the file system is also marked as corrupt.

The CORRUPT column indicates whether the file system needs the fsck or acfschkdsk command run on it. See “fsck” and “acfschkdsk”.

See Also:

Oracle Database Reference for information about the V\$ASM_FILESYSTEM view

[Example 9](#) shows information displayed from the V\$ASM_VOLUME view for volumes contained in the DATA disk group.

See Also:

Oracle Database Reference for information about the V\$ASM_VOLUME view

[Example 10](#) shows information displayed from the V\$ASM_VOLUME_STAT view for volumes contained in the DATA disk group. The BYTES_READ column contains the total number of bytes read for the volume. The BYTES_WRITTEN column contains the total number of bytes written for the volume.

See Also:

Oracle Database Reference for information about the V\$ASM_VOLUME_STAT view

[Example 11](#) shows tag names for the /acfsmounts/acfs1 file system displayed from the V\$ASM_ACFSTAG view.

See Also:

Oracle Database Reference for information about the V\$ASM_ACFSTAG view

Example 1 Viewing encryption information in V\$ASM_ACFS_ENCRYPTION_INFO

```
SELECT SUBSTR(fs_name,1,24) FILESYSTEM, SUBSTR(vol_device,1,20) DEVICE, set_status,
       enabled_status, algorithm, key_length, last_rekey_time FROM V$ASM_ACFS_ENCRYPTION_INFO;
```

FILESYSTEM	DEVICE	SET_STA	ENABLED_	ALGORIT	KEY_LEN	LAST_REKE
/acfsmounts/acfs1	/dev/asm/volume1-228	YES	ENABLED	AES	192	

Example 2 Viewing security information in V\$ASM_ACFS_SECURITY_INFO

```
SELECT SUBSTR(fs_name,1,24) FILESYSTEM, SUBSTR(vol_device,1,20) DEVICE, prepared_status,
       enabled_status FROM V$ASM_ACFS_SECURITY_INFO;
```

FILESYSTEM	DEVICE	PREPARE	ENABLED_
/acfsmounts/acfs1	/dev/asm/volume1-228	YES	ENABLED

Example 3 Viewing security rules information in V\$ASM_ACFS_SEC_RULE

```
SELECT SUBSTR(rule_name,1,24) rule, SUBSTR(rule_type,1,12) type,
       SUBSTR(rule_value,1,16) value, SUBSTR(fs_name,1,24) filesystem
FROM V$ASM_ACFS_SEC_RULE;
```

RULE	TYPE	VALUE	FILESYSTEM
medHistRule1a	TIME	22:00:00	/acfsmounts/acfs1
medHistRule1c	TIME	08:00:00	/acfsmounts/acfs1
medHistRule1b	USERNAME	medMaintenance	/acfsmounts/acfs1
medHistRule1d	USERNAME	medBrowse	/acfsmounts/acfs1
SYSTEM_RULE_Auditor	GROUPNAME	myaudit_mgr_grp	/acfsmounts/acfs1
SYSTEM_RULE_AuditManager	GROUPNAME	myauditor_grp	/acfsmounts/acfs1
SYSTEM_RULE_Always	TIME	00:00:00	/acfsmounts/acfs1

Example 4 Viewing security ruleset information in V\$ASM_ACFS_SEC_RULESET

```
SELECT SUBSTR(ruleset_name,1,36) ruleset, ruleset_option r_option, SUBSTR(fs_name,1,24)
filesystem
FROM V$ASM_ACFS_SEC_RULESET;
```

RULESET	R_OPTION	FILESYSTEM
medRuleSet1	ALL_TRUE	/acfsmounts/acfs1
medRuleSet2	ALL_TRUE	/acfsmounts/acfs1
SYSTEM_RULESET_Auditor	ALL_TRUE	/acfsmounts/acfs1
SYSTEM_RULESET_AuditManager	ALL_TRUE	/acfsmounts/acfs1
SYSTEM_RULESET_AuditMgr_Auditor	ANY_TRUE	/acfsmounts/acfs1
SYSTEM_RULESET_AlwaysDeny	ANY_TRUE	/acfsmounts/acfs1

Example 5 Viewing security ruleset information in V\$ASM_ACFS_SEC_RULESET_RULE

```
SELECT SUBSTR(ruleset_name,1,36) ruleset, substr(rule_name,1,24) rule,
SUBSTR(fs_name,1,36) filesystem FROM V$ASM_ACFS_SEC_RULESET_RULE;
```

RULESET	RULE	FILESYSTEM
medRuleSet1	medHistRule1a	/acfsmounts/acfs1
medRuleSet1	medHistRule1b	/acfsmounts/acfs1
medRuleSet2	medHistRule1c	/acfsmounts/acfs1
medRuleSet2	medHistRule1d	/acfsmounts/acfs1
SYSTEM_RULESET_Auditor	SYSTEM_RULE_Auditor	/acfsmounts/acfs1
SYSTEM_RULESET_AuditManager	SYSTEM_RULE_AuditManager	/acfsmounts/acfs1
SYSTEM_RULESET_AuditMgr_Auditor	SYSTEM_RULE_Auditor	/acfsmounts/acfs1
SYSTEM_RULESET_AuditMgr_Auditor	SYSTEM_RULE_AuditManager	/acfsmounts/acfs1
SYSTEM_RULESET_AlwaysDeny	SYSTEM_RULE_Always	/acfsmounts/acfs1

Example 6 Viewing snapshot information in V\$ASM_ACFSSNAPSHOTS

```
SELECT SUBSTR(FS_NAME,1,24) FILESYSTEM, SUBSTR(VOL_DEVICE,1,22) DEVICE,
SUBSTR(SNAP_NAME,1,12) SNAPSHOT, CREATE_TIME TIME, SUBSTR(PARENT,1,10) PARENT,
SUBSTR(TYPE,1,4) TYPE FROM V$ASM_ACFSSNAPSHOTS;
```

FILESYSTEM	DEVICE	SNAPSHOT	TIME	PARENT	TY
/acfsmounts/acfs1	/dev/asm/volume1-229	snprw	13-MAR-12	NULL	RW
/acfsmounts/acfs1	/dev/asm/volume1-229	snprw_child	13-MAR-12	snprw	RW
/acfsmounts/acfs2	/dev/asm/volume2-321	snapro	13-MAR-12	NULL	RO

Example 7 Viewing volume information with V\$ASM_ACFSVOLUMES

```
SELECT fs_name, vol_device, primary_vol, total_mb, free_mb FROM V$ASM_ACFSVOLUMES;
```

FS_NAME	VOL_DEVICE	PRIMARY_VOL	TOTAL_MB	FREE_MB
/acfsmounts/acfs1	/dev/asm/volume1-228	TRUE	1024000	578626.522
/acfsmounts/acfs2	/dev/asm/volume2-375	TRUE	1024000	685761.463
...				

Example 8 Viewing volume information with V\$ASM_FILESYSTEM

```
SELECT fs_name, available_time, block_size, state, corrupt FROM V$ASM_FILESYSTEM;
```

FS_NAME	AVAILABLE	BLOCK_SIZE	STATE	CORRUPT
/acfsmounts/acfs1	19-JUL-09	4	AVAILABLE	FALSE
/acfsmounts/acfs2	19-JUL-09	4	AVAILABLE	FALSE

Example 9 Viewing volume information with V\$ASM_VOLUME

```
SELECT dg.name AS diskgroup, v.volume_name, v.volume_device, v.mountpath
FROM V$ASM_DISKGROUP dg, V$ASM_VOLUME v
```

```
WHERE dg.group_number = v.group_number and dg.name = 'DATA';
```

DISKGROUP	VOLUME_NAME	VOLUME_DEVICE	MOUNTPATH
DATA	VOLUME1	/dev/asm/volume1-228	/acfsmounts/acfs1
DATA	VOLUME2	/dev/asm/volume2-375	/acfsmounts/acfs2

Example 10 Viewing volume information with V\$ASM_VOLUME_STAT

```
SELECT dg.name AS diskgroup, v.volume_name, v.bytes_read, v.bytes_written
FROM V$ASM_DISKGROUP dg, V$ASM_VOLUME_STAT v
WHERE dg.group_number = v.group_number and dg.name = 'DATA';
```

DISKGROUP	VOLUME_NAME	BYTES_READ	BYTES_WRITTEN
DATA	VOLUME1	12370105856	43510272
DATA	VOLUME2	2685728	32201504

Example 11 Viewing tag name information with V\$ASM_ACFSTAG

```
SELECT SUBSTR(TAG_NAME,1,8) TAG_NAME, SUBSTR(FS_NAME,1,20) FS_NAME,
SUBSTR(PATH_NAME,1,42) PATH_NAME FROM V$ASM_ACFSTAG WHERE TAG_NAME='tag5';
```

TAG_NAME	FS_NAME	PATH_NAME
tag5	/acfsmounts/acfs1	/acfsmounts/acfs1/d1/d2/d3/d4/d5/f6
tag5	/acfsmounts/acfs1	/acfsmounts/acfs1/d1/d2/d3/d4/d5
tag5	/acfsmounts/acfs1	/acfsmounts/acfs1/d1/d2/d3/d4
tag5	/acfsmounts/acfs1	/acfsmounts/acfs1/d1/d2/d3
tag5	/acfsmounts/acfs1	/acfsmounts/acfs1/d1/d2
tag5	/acfsmounts/acfs1	/acfsmounts/acfs1/d1
tag5	/acfsmounts/acfs1	/acfsmounts/acfs1/f1
tag5	/acfsmounts/acfs1	/acfsmounts/acfs1

Oracle ACFS Support for Oracle Database File Mapping Views

Note:

This feature is available starting with Oracle Database 12c Release 1 (12.1.0.2).

Oracle ACFS supports Oracle Database file mapping views to the Oracle ASM device level. For information about file mapping to Oracle ASM files, refer to [“Oracle Database File Mapping for Oracle ASM Files”](#).

The following database mapping views are supported by Oracle ACFS:

- V\$MAP_FILE
- V\$MAP_FILE_EXTENT
- V\$MAP_ELEMENT
- V\$MAP_FILE_IO_STACK

These V\$MAP views are only refreshed by executing the procedure `DBMS_STORAGE_MAP.MAP_ALL`. The Oracle ACFS file mapping interface does not utilize the external `fmpu1` process or its supporting libraries.

Note:

- Oracle ACFS does not provide support for Oracle Database file mapping on Windows.
 - Oracle ACFS does not provide support for the V\$MAP_SUBELEMENT view.
-
-

Before running any queries on the V\$MAP views, ensure that the FILE_MAPPING initialization is set to TRUE, then run the DBMS_STORAGE_MAP.MAP_ALL procedure to build the mapping information for the entire I/O subsystem associated with the database. For example, connect as SYSDBA to the database instance and run the following:

```
SQL> ALTER SYSTEM SET file_mapping=true;

SQL> EXEC DBMS_STORAGE_MAP.MAP_ALL(10000);
```

The SQL statements in [Example 12](#) to [Example 15](#) are run from the Oracle Database instance. [Example 12](#) displays information from the V\$MAP_ELEMENT view.

[Example 13](#) displays information from the V\$MAP_FILE view.

[Example 14](#) displays the element offset versus file offset information for each extent with V\$MAP_FILE_EXTENT, specifying FILE_MAP_IDX equal to 4, which is the file map index of the /dbdata/orcl/users01.dbf file.

[Example 15](#) displays information from V\$MAP_FILE_IO_STACK specifying FILE_MAP_IDX equal to 4. The V\$MAP_FILE_IO_STACK view is similar to V\$MAP_FILE_EXTENT, but the display groups contiguous extents which are on the same device or element and of the same size.

See Also:

- *Oracle Database Administrator's Guide* for information about the Oracle Database File Mapping Interface
 - *Oracle Database Reference* for details about the V\$MAP views
-
-

Example 12 Viewing Oracle ASM information with V\$MAP_ELEMENT

```
SQL> SELECT ELEM_NAME, ELEM_IDX, ELEM_TYPE, ELEM_SIZE, ELEM_DESCR
        FROM V$MAP_ELEMENT;
```

ELEM_NAME	ELEM_IDX	ELEM_TYPE	ELEM_SIZE	ELEM_DESCR
+/dev/xvddl	0	ASMDISK	117184512	TEST_0001
+/dev/xvdc1	1	ASMDISK	117184512	TEST_0000

Example 13 Viewing Oracle ACFS Data File Information with V\$MAP_FILE

```
SQL> SELECT FILE_NAME, FILE_MAP_IDX, FILE_TYPE, FILE_STRUCTURE, FILE_SIZE,
        FILE_NEXTS FROM V$MAP_FILE WHERE REGEXP_LIKE(FILE_NAME, '*users01.dbf');
```

FILE_NAME	FILE_MAP_IDX	FILE_TYPE	FILE_STRU	FILE_SIZE	FILE_NEXTS
/dbdata1/orcl/users01.dbf	4	DATAFILE	FILE	10256	41

Example 14 Viewing Element and File Offset Information with V\$MAP_FILE_EXTENT

```
SQL> SELECT FILE_MAP_IDX, EXT_NUM, EXT_ELEM_OFF, EXT_SIZE, EXT_FILE_OFF,
           EXT_TYPE, ELEM_IDX FROM V$MAP_FILE_EXTENT WHERE FILE_MAP_IDX=4;
```

FILE_MAP_IDX	EXT_NUM	EXT_ELEM_OFF	EXT_SIZE	EXT_FILE_OFF	EXT_TY	ELEM_IDX
4	0	58105664	192	0	DATA	0
4	1	58154752	256	192	DATA	1
4	2	58089472	256	448	DATA	0
...						
4	39	58140928	256	9920	DATA	1
4	40	58108160	88	10176	DATA	0

41 rows selected.

Example 15 Viewing Extent Information With V\$MAP_FILE_IO_STACK

```
SQL> SELECT FILE_MAP_IDX, ELEM_IDX, CU_SIZE, STRIDE, NUM_CU, ELEM_OFFSET,
           FILE_OFFSET FROM V$MAP_FILE_IO_STACK WHERE FILE_MAP_IDX=4;
```

FILE_MAP_IDX	ELEM_IDX	CU_SIZE	STRIDE	NUM_CU	ELEM_OFFSET	FILE_OFFSET
4	0	256	1024	10	58089472	448
4	0	192	0	1	58105664	0
4	0	256	1024	9	58105856	960
4	0	88	0	1	58108160	10176
4	1	256	1024	10	58138624	704
4	1	256	1024	10	58154752	192

6 rows selected.

Administering Oracle ACFS with Oracle Enterprise Manager

This chapter describes how to administer Oracle Automatic Storage Management Cluster File System (Oracle ACFS) with Oracle Enterprise Manager Cloud Control.

All Oracle ASM administration tasks begin with the Oracle Automatic Storage Management home page in Oracle Enterprise Manager Cloud Control. For information about the Oracle ASM home page and how to access that page, see “[Accessing the Oracle Automatic Storage Management Home Page](#)”.

For information about using command-line tools to administer Oracle ACFS file systems, see [Managing Oracle ACFS with Command-Line Tools](#). For information about the basic steps for creating Oracle ACFS file systems, see “[Basic Steps to Manage Oracle ACFS Systems](#)”.

This chapter contains the following topics:

- [Managing Oracle ACFS File Systems and Volumes with Oracle Enterprise Manager](#)
- [Managing Oracle ACFS Snapshots with Oracle Enterprise Manager](#)
- [Managing Security Features with Oracle Enterprise Manager](#)
- [Managing Encryption Features with Oracle Enterprise Manager](#)
- [Managing Tagging Features with Oracle Enterprise Manager](#)

Note:

To manage or monitor Oracle ACFS file systems or volumes that are located on nodes in an Oracle Flex ASM configuration, you must connect to the Oracle ASM proxy instance instead of the local Oracle ASM instance. For information about Oracle Flex ASM, refer to “[Managing Oracle Flex ASM](#)”.

Managing Oracle ACFS File Systems and Volumes with Oracle Enterprise Manager

This section discusses how to manage Oracle ACFS file systems and volumes systems with Oracle Enterprise Manager Cloud Control.

This section contains the following topics:

- [Creating Oracle ACFS File Systems and Volumes](#)
- [Viewing and Modifying Oracle ACFS Volumes and File Systems](#)

For more information about Oracle ACFS file systems and volumes, refer to [“About Oracle ACFS”](#).

See Also:

- *Oracle Enterprise Manager Cloud Administration Guide*
 - *Oracle Enterprise Manager Administration*
-
-

Creating Oracle ACFS File Systems and Volumes

To create an Oracle ACFS volume, perform the following steps.

1. Access the **Disk Groups** page from the Oracle ASM home page.
For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).
2. Click the **Volumes** link in the **General** tab of the **Disk Group** page. See [Figure 4](#).
3. Click **Create** in the **Volumes** tab of the **Disk Group** page.

The **Create ASM Volume** page displays, shown in [Figure 1](#).

Enter the volume name, disk group name that contains the volume, and the initial size of the volume.

You can also select the redundancy setting for the volume and the region settings for primary and mirror extents. For information about redundancy settings, refer to [“Mirroring, Redundancy, and Failure Group Options”](#). For information about hot and cold disk regions, refer to [“Intelligent Data Placement”](#). For information about creating a volume with the ASMCMD `volcreate` command, refer to [“ASMCMD Volume Management Commands”](#).

[Figure 1](#) shows the **Oracle ASM Create ASM Volume** page.

Figure 1 Oracle ACFS Create ASM Volume Page

Create ASM Volume Show Command Cancel Ok

Disk Group: DATA Disk Group Usable Free Space (GB): 3.3027
Volume Allocation Unit (MB): 256

* Volume:

* Size: GB
Volume size will be adjusted to be in multiples of the Volume Allocation Unit.

Redundancy:

Stripe Width (KB): 128
Stripe Columns: 4

Regions

Specify the regions that the primary and mirror extents should be written to based on access pattern. Place frequently accessed data in the hot region, which is in the outermost tracks. The hot region has higher bandwidth and can provide improved I/O latency

Primary: Hot Cold
Mirror: Hot Cold

TIP If the data is frequently accessed and mostly read only, put the primary extents in the hot region and mirror extents in the cold region. If the data is frequently accessed and updated, put both primary and mirror extents in the hot region

Show Command Cancel Ok

To create an Oracle ACFS file system on a volume in a disk group, perform the following steps.

1. Access the **Volumes** tab of the **Disk Group** page. See [Figure 4](#).
2. Select an existing volume in the disk group and click **Create ASM Cluster File System**.

The compatibility parameters `COMPATIBLE.ASM` and `COMPATIBLE.ADVM` must be set to 11.2 or higher for the disk group. See [“Disk Group Compatibility Attributes”](#).

3. On the **Create ASM Cluster File System** page, enter the information to create a file system. You can optionally register and mount the file system.

You must enter the volume name. You can enter an optional volume label.

You can optionally choose to register and mount the file system when it is created. Select a mount point from available directories.

Enter the host credentials needed to run the command when prompted. To register or mount a file system, you need root or administrator privileges. For information about the registry process, see [“About the Oracle ACFS Mount Registry”](#).

After a directory has been selected, click **Show Command** to have Oracle Enterprise Manager generate the commands that you can run at an operating system prompt. Examples of commands on a Linux system are:

```
/sbin/mkfs -t acfs -b 4k /dev/asm/volume1-361
/sbin/acfsutil registry -f -a /dev/asm/volume1-361 /oracle/acfsmounts/acfs2
/bin/mount -t acfs -rw /dev/asm/volume1-361 /oracle/acfsmounts/acfs2
```

You can also generate the commands to register or mount an Oracle ACFS file system on the **ASM Cluster File System** tab.

Viewing and Modifying Oracle ACFS Volumes and File Systems

To view and modify information about Oracle ACFS file systems, click the **ASM Cluster File System** link in the Oracle ASM home page.

[Figure 2](#) shows the **ASM Cluster File System** tab in Oracle Enterprise Manager. This tab lists all of the Oracle ACFS associated with the Oracle ASM instance.

On this page, you can choose to mount, dismount, delete, create snapshot, view content, register, and deregister a selected file system. In addition, you can create a file system, mount all file systems, or dismount all file systems.

For each Oracle ACFS, the columns provide information for Mount Point, Availability, State, Snapshots, Used (%), Used (GB), Size (GB), Allocated Space, Redundancy, Volume, and Disk Group. Redundancy, Volume, and Disk Group columns are on the far right of the page and are not shown in the illustration. The mount point, snapshots, volume, and disk group are provided as links to further information.

Figure 2 Oracle ACFS Page

To view information about a specific volume, click the volume name in the **Volume** column on the **ASM Cluster File System** page to display the **General** tab of the **ASM Volumes** page.

To view information about a file system, click the link in the **Mount Point** column on the **ASM Cluster File System** page.

Figure 3 shows the **General** tab of the **ASM Cluster File System** page.

Figure 3 Oracle ACFS General Page

To view information about a disk group for an Oracle ACFS, click the disk group name in the **Disk Group** column on the **ASM Cluster File System** page. The **General** tab of the **Disk Group** page displays as shown in Figure 6 .

To view information about volumes in a disk group, click the **Volumes** tab at the top of the **Disk Group** page.

Figure 4 shows the Oracle ACFS Volume page.

Figure 4 Oracle ACFS Volume Page

Disk Group: DATA

General Performance Templates Files Access Control **Volumes**

Create Enable All Disable All

ASM volumes are typically formatted with ASM Cluster File Systems, which you can use to store non-database files such as executables, Oracle trace files and alert logs, application configuration files, and so on.

Enable Disable Edit Create ASM Cluster File System View Delete

Select All | Select None

Select	Volume	Volume Device	State	Usage	Mount Point	Size (GB)	Allocated Space (GB)	Redundancy
<input type="checkbox"/>	VOLUME1	/dev/asm/volume1-401	ENABLED	ACFS	/acfsmounts/acfs1	1	2.0029	Mirror
<input type="checkbox"/>	VOLUME2	/dev/asm/volume2-401	ENABLED	Not Specified		1	2.0029	Mirror

Managing Oracle ACFS Snapshots with Oracle Enterprise Manager

This section describes how to manage snapshots with Oracle Enterprise Manager.

- [Creating_ Modifying_ and Viewing Snapshots](#)
- [Converting Snapshots Between Read-Only and Read-Write](#)
- [Creating Child Snapshots from Existing Snapshots](#)

For more information about Oracle ACFS snapshots, refer to “[About Oracle ACFS Snapshots](#)”.

Creating, Modifying, and Viewing Snapshots

To view and modify information about existing snapshots or create snapshots for a file system, perform the following steps.

1. Click the **ASM Cluster File System** tab on the Oracle ASM home page
2. Click a mount point link in the **Mount Point** column as shown in [Figure 2](#)
3. Click the **Snapshots** tab, shown in [Figure 5](#).

Optionally, you can click a number link for existing snapshots in the **Snapshots** column on the **ASM Cluster File System** page to display the **Snapshots** page.

On the **Snapshots** page, you can create snapshots or search for and display specific snapshots. To search for a snapshot, enter a name with optional wildcard characters in the search field then click **Search**.

Figure 5 Oracle ACFS Snapshots Tab

ASM Cluster File System: /acfsmounts/acfs1

General **Snapshots** Security/Encryption

Summary

A snapshot is a space efficient point-in-time copy of the file system. It can be used as a backup source to recover accidentally deleted or modified files, or for data mining and report applications.

Number of Snapshots 1
 Last Snapshot Creation Time Jan 16, 2013 3:01:30 PM PST
 Space Used by Snapshots (MB) 0.0312
 File System Free Space (GB) 0.8982

Snapshots

Search

To narrow down the search results or to search for a specific snapshot, enter a search string in the Snapshot name field and click Search. To display all the ACFS snapshots for the selected ACFS filesystem, clear the search field and click Search.

Name

TIP To return exact or case-sensitive matches, double quote the search strings. You can use the wildcard symbol (% , *) in a double-quoted string.

Select All | Select None

Select	Name	Parent Name	Creation Time	Attribute
<input type="checkbox"/>	snapshot_20130116_145614		Jan 16, 2013 3:01:30 PM PST	Read Only

To create a snapshot, perform the following steps.

1. Click **Create** in the **Snapshots** page.

[Figure 6](#) shows the **Create Snapshot** page.

2. Complete the information on the page.

Accept the default snapshot name, or provide a name. Optionally, you can choose to delete the oldest snapshot.

3. When you have completed the screen, you can click **OK** to run the command, or click **Show Command** to view the generated command.

For example, the following is a generated command for creating a snapshot:

```
/sbin/acfsutil snap create "snapshot_20090702_142135" /oracle/acfsmounts/acfs1
```

To run the generated command, you need the appropriate privileges on the host computer. Oracle Enterprise Manager prompts you to enter host credentials if they have not been set up.

You can also open a Telnet session from the **Create Snapshot** page to manually enter the generated operating system command.

Figure 6 Oracle ACFS Create Snapshot Page

Create Snapshot on ASM Cluster File System: /acfsmounts/acfs1

Show Command Cancel Ok

Number of Snapshots: 0
Total Free Space (GB): 0.8982

The Create Snapshot operation creates a point-in-time copy of the ASM Cluster File System. Snapshots are always mounted and available. The snapshots are created in the `._ACFS/snaps` directory of the file system with the snapshot name as the directory name.

* Snapshot Name:

Attribute: Read Only Read Write

Related Links
[Open Telnet Session](#)

Show Command Cancel Ok

To drill down in a snapshot directory, click the snapshot name in the **Snapshots** page to display the **Search and List Directory** page.

Converting Snapshots Between Read-Only and Read-Write

You can use edit snapshot to convert the snapshot attribute between Read Only and Read Write. To edit a snapshot, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.
2. Click the file or directory in which you want to edit a snapshot.
Enterprise Manager displays ASM Cluster File System page.
3. Click the **Snapshots** tab.
4. Select the snapshot you want to edit, then click **Edit**.
The Snapshot page displays.
5. Change the Attribute. You can choose **Read Only** or **Read Write**.
6. Click **OK**.

Creating Child Snapshots from Existing Snapshots

Use the Create Child snapshot operation to create a point-in-time copy of an existing Oracle ACFS snapshot. Future changes to the parent snapshot are not inherited by the child snapshot. To create a child snapshot of an existing snapshot, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.
2. Click the file or directory Mount Point in which you want to create a child snapshot.
Enterprise Manager displays ASM Cluster File System page.
3. Click the **Snapshots** tab.
4. Select the parent snapshot you want to use to create a child snapshot, then click **Create Child**.

The Create Child Snapshot on ASM Cluster File System page displays.

5. The Snapshot Name field is automatically populated with a default child snapshot name. You can replace the name with a name you designate.
6. Set the Attribute to **Read Only** or **Read Write**.
7. Optionally you can turn on the option to delete the oldest snapshot by turning on the delete option. Oracle Enterprise Manager tabulates the number of remaining snapshots before the maximum limit is reached.
8. Click **OK** to create the child snapshot.

Oracle Enterprise Manager returns to the Snapshots tab where you can see the new snapshot with its Parent Name listed in the table.

Managing Security Features with Oracle Enterprise Manager

This section describes how to manage security with Oracle Enterprise Manager.

- [Initializing Oracle ACFS Security](#)
- [Preparing an Oracle ACFS For Security](#)
- [Undoing Oracle ACFS Security](#)
- [Enabling Security on Oracle ACFS](#)
- [Disabling Security on Oracle ACFS](#)
- [Viewing Security Status](#)
- [Adding an Oracle ACFS Security Administrator](#)
- [Changing an Oracle ACFS Security Administrator Password](#)
- [Deleting an Oracle ACFS Security Administrator](#)
- [Viewing Oracle ACFS Security Administrators](#)
- [Creating a Rule](#)
- [Cloning a Rule](#)
- [Editing a Rule](#)
- [Deleting a Rule](#)
- [Searching For and Viewing Rules](#)
- [Creating a Ruleset](#)
- [Cloning a Ruleset](#)
- [Editing a Ruleset](#)
- [Deleting a Ruleset](#)
- [Searching For and Viewing Rulesets](#)
- [Creating a Realm](#)
- [Cloning a Realm](#)

- [Adding Objects to a Realm](#)
- [Deleting Objects from a Realm](#)
- [Deleting a Realm](#)
- [Viewing Realms](#)

For more information about Oracle ACFS security, refer to “[Oracle ACFS Security](#)”.

Initializing Oracle ACFS Security

Oracle ACFS security provides a unified security infrastructure that allows users to define security policies and groups for accessing file system objects. Oracle ACFS encryption allows users to store data on disk in an encrypted format. To initialize Oracle ACFS security, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.
For information about the Oracle ASM home page and how to access that page, see “[Accessing the Oracle Automatic Storage Management Home Page](#)”.
2. Click a mount point in the list.
3. Click the **Security/Encryption** to display the Security and Encryption section.
4. In the **Security Configuration** section, you can click **Configuration**, **Rules**, **Rulesets**, and **Realms** under **Security** to display various options as shown in [Figure 7](#).
5. If Oracle ACFS security is not initialized in the cluster, the **Initialize Security** button displays on the page. Click the button to initialize Oracle ACFS security. This operation needs to be performed only once in the cluster. On this page, you can also prepare security for the file system.

Figure 7 Oracle ACFS Security Configuration Page

The screenshot displays the Oracle ACFS Security Configuration page for the ASM Cluster File System: /acfsmounts/acfs1. The page is divided into several sections:

- General Information:** Shows the file system path and tabs for General, Snapshots, and Security/Encryption.
- Security Configuration:**
 - Current Configuration:** Prepared Status: Prepared; Enabled Status: Enabled.
 - Edit Configuration:** Actions: Prepare Security (dropdown), Go (button). A link to "View File Security and Encryption Properties" is also present.
- ACFS Security Access Control Workflow:** A diagram illustrating the flow of security access control:
 - Ruleset - HR_Staff:** Contains three rules:
 - Rule 1: John has Access
 - Rule 2: HR has Access
 - Rule 3: Access from 9am - 5pm
 - Access:** Assign Read access to Ruleset HR Staff on Realm HR.
 - Realm - HR:** Contains objects such as benefits.xml, Company, HR, Payroll, and Review Documents.

Preparing an Oracle ACFS For Security

To prepare an Oracle ACFS for security, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click the **Mount Point** of the file system for which you want to prepare security.

Enterprise Manager displays the ASM Cluster File System page for that mount point.

3. Click the **Security/Encryption** tab to display the Security Overview section. This page shows the security details for the current file system.

4. From the Actions menu, click **Prepare Security**.

Undoing Oracle ACFS Security

To undo preparation for Oracle ACFS security, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click the **Mount Point** of the file system for which you want to unprepare security.

Enterprise Manager displays the ASM Cluster File System page for that mount point.

3. Click the **Security/Encryption** tab to display the Security Overview section. This page shows the security details for the current file system.

4. From the Actions menu, click **Unprepare Security**.

Enabling Security on Oracle ACFS

To enable security on Oracle ACFS, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click the **Mount Point** of the file system for which you want to enable security.

Enterprise Manager displays the ASM Cluster File System page for that mount point.

3. Click the **Security/Encryption** tab to display the Security Overview section. This page shows the security details for the current file system.

4. From the Actions menu, click **Enable Security**.

Disabling Security on Oracle ACFS

To disable security on an Oracle ACFS, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click the **Mount Point** of the file system for which you want to disable security.

Enterprise Manager displays the ASM Cluster File System page for that mount point.

3. Click the **Security/Encryption** tab to display the Security Overview section. This page shows the security details for the current file system.

4. From the Actions menu, click **Disable Security**.

Viewing Security Status

To view security status, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click **Show Security and Encryption** to display the Security and Encryption section.

The section displays the mount points and the security and encryption settings for each.

Adding an Oracle ACFS Security Administrator

To add an Oracle ACFS security administrator, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click **Show Security and Encryption** to display the **Security and Encryption** section.

3. The list of Oracle ACFS security administrators in this cluster is displayed. Click the **Create** button. The **Create Administrator** page is displayed.

4. Enter the input details and click **OK**.

Changing an Oracle ACFS Security Administrator Password

To change an Oracle ACFS security administrator password, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click **Show Security and Encryption** to display the **Security and Encryption** section.
3. The list of Oracle ACFS security administrators in this cluster is displayed. Select a security administrator and click the **Change Password** button. The **Change Administrator Password** page is displayed.
4. Enter the input details and click **OK**.

Deleting an Oracle ACFS Security Administrator

To delete an Oracle ACFS security administrator, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click **Show Security and Encryption** to display the **Security and Encryption** section.
3. The list of Oracle ACFS security administrators in this cluster is displayed. Click the **Delete** button.

Viewing Oracle ACFS Security Administrators

To view Oracle ACFS security administrators, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click **Show Security and Encryption** to display the **Security and Encryption** section.
3. The list of Oracle ACFS security administrators in this cluster is displayed.

Creating a Rule

Rules are created in a file system and can be added to one or more rulesets, which can then be applied on an Oracle ACFS realm. Rules can also be cloned within the same file system or across file systems.

To create a rule, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Rules**.
The list of rules in the mount point is displayed.
5. Click **Create**. The Create Rule page displays along with the available rule options.
6. Enter the input details and click **OK**.

Cloning a Rule

Rules can be cloned within the same mount point or across mount points. To clone a rule, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.
For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).
2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Rules**.
The list of rules in the mount point is displayed.
5. Click **Clone**. The Clone Rule page is displayed with the available rule options.
6. Enter the input details and click **OK**.

Editing a Rule

You can modify values and options for an existing rules. Rule types cannot be changed. To edit a rule, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.
For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).
2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Rules**.
The list of rules in the mount point is displayed.
5. Select a rule and click **Edit**.
6. Edit the input details and click **OK**.

Deleting a Rule

You can delete a rule so it no longer is used to enforce security on realms. To delete a rule, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Rules**.

The list of rules in the mount point is displayed.

5. Select a rule and click the **Delete Rule** button.

Searching For and Viewing Rules

You can view or search the list of rules on a mount point, including the details of each rule. To search for and view rules, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the **Security** section, click **Rules**.

The list of rules in the file system is displayed as shown in [Figure 8](#).

Figure 8 Oracle ACFS Security Rules Page

ASM Cluster File System: /acfsmounts/acfs1

General Snapshots Security/Encryption

Security

Configuration

Rules (7)

Rulesets (6)

Realms (5)

Encryption

Configuration

Rules

A rule is a Boolean expression that evaluates to true or false based on the parameter on which the rule is based. An option of "allow" or "deny" can be associated with each rule.

Search Rule Name

Rule Name	Rule Type	Rule Value1	Rule Value2	Rule Option
medHistRule1a	TIME	22:00:00	02:00:00	✓
medHistRule1c	TIME	08:00:00	09:00:00	✗
medHistRule1b	USERNAME	oracle		✓
medHistRule1d	USERNAME	oracle		✗
SYSTEM_RULE_Auditor	GROUPNAME	g527		✓
SYSTEM_RULE_AuditMe	GROUPNAME	g527		✓
SYSTEM_RULE_Always	TIME	00:00:00	23:59:59	✓

✓ Allow ✗ Deny

Creating a Ruleset

You can create a ruleset which is a collection of one or more rules that you can associate with a command rule for realm authorization. A ruleset evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (All True or Any True). Rulesets cannot be applied on an Oracle ACFS security realm directly; they are always associated with a Command Rule, which are then applied on a realm to enforce security. To create a ruleset, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Rulesets**.

The list of rulesets in the mount point is displayed.

5. Click **Create**. The Create Ruleset page is displayed along with the available ruleset options.
6. Enter the input details and click **OK**.

Cloning a Ruleset

Rulesets can be cloned within the same mount point or across mount points. To clone a ruleset, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Rulesets**.

The list of rulesets in the mount point is displayed.

5. Click the ruleset you want to clone then click **Clone**. The Clone Ruleset page is displayed along with the available ruleset options.
6. Enter input details and click **OK**.

Editing a Ruleset

You can add or delete rules to or from a Ruleset. You can also edit the Ruleset options. To edit a ruleset, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Rulesets**.

The list of rulesets in the mount point is displayed.

5. Select a ruleset and click **Edit**. The Edit Ruleset page is displayed along with all the ruleset values.
6. Edit the ruleset details and click **OK**.

Deleting a Ruleset

Deleted rulesets are no longer used to enforce security on realms. To delete a ruleset, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.

3. Click the **Security/Encryption** tab.
4. In the Security section, click **Rulesets**.

The list of rulesets in the mount point is displayed.

5. Select a ruleset and click **Delete**.

Searching For and Viewing Rulesets

A ruleset is a collection of one or more rules that you can associate with a command rule for realm authorization. A ruleset evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (All True or Any True). Enterprise Manager enables you to view and search the list of rulesets applied on an Oracle ACFS mount point, including the details of each ruleset. To search for and view rulesets, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.
For information about the Oracle ASM home page and how to access that page, see "[Accessing the Oracle Automatic Storage Management Home Page](#)".
2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the **Security** section, click **Rulesets**.

The list of rulesets in the file system is displayed as shown in [Figure 9](#).

Figure 9 Oracle ACFS Security Rulesets Page

The screenshot shows the Oracle ACFS Security Rulesets page. The page title is "ASM Cluster File System: /acfsmounts/acfs1". The "Security/Encryption" tab is selected. The "Rulesets" section is active, displaying a list of rulesets. The list has columns for "Ruleset Name", "Rules", and "Evaluation Option".

Ruleset Name	Rules	Evaluation Option
medRuleSet1	medHistRule1 a,medHistRule1 b	ALL_TRUE
SYSTEM_RULESET_AlwaysDeny	SYSTEM_RULE_Always	ANY_TRUE
SYSTEM_RULESET_AuditManager	SYSTEM_RULE_AuditManager	ALL_TRUE
SYSTEM_RULESET_AuditMgr_Auditor	SYSTEM_RULE_AuditManager,SYSTEM_RULE_Auditor	ANY_TRUE
SYSTEM_RULESET_Auditor	SYSTEM_RULE_Auditor	ALL_TRUE
medRuleSet2	medHistRule1 c,medHistRule1 d	ALL_TRUE

Creating a Realm

Oracle ACFS Security realms provide the capability to classify file system objects into functional groups to provide fine-grained access control to data stored in these objects.

Realms are created at the file system level. To enforce security on the file objects in a realm, a ruleset is associated with a command rule which is then applied on the realm.

To create a realm, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Realms**.
5. Click **Create**. The Create Realm wizard displays along with the available realm options.
6. Enter the input details and click **OK**.

Cloning a Realm

Cloning a realm creates a new realm with all the objects of which the cloned realm consists. To clone a realm, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click a **Mount Point**. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Realms**. The list of realms in the mount point is displayed.
5. Select a realm and click **Clone Realm**. The **Clone Realm** page is displayed along with the available realm options. A realm can be cloned within the same mount point with a different name or across mount points. You can choose the properties; such as users, groups, and encryption; to propagate to the cloned realm.
6. Enter the input details and click **OK**.

Adding Objects to a Realm

Once a realm is created, you can add objects to a realm. To add objects to a realm, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click the **Mount Point** that contains the realm to which you want to add objects. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Realms**. The list of realms in the mount point is displayed.
5. Select a realm and click the **Edit** button. The Edit Realm wizard displays.
6. Click **Next** to move to the Realm Objects page where you can click **Add** to add objects to the realm.
7. Click **Done**.

Deleting Objects from a Realm

You can delete various objects from a realm. If a file or directory is removed from a realm, it is not subjected to security or encryption that is enforced on the realm. If a command rule is deleted from a realm, it is not evaluated while enforcing security on the realm. The command rule still continues to exist for use in other realms. If an encryption object is removed, it disables encryption on the realm and results in decryption of all encrypted files in the realm.

To delete an object from a realm, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click the **Mount Point** that contains the realm from which you want to delete objects. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Realms**. The list of realms in the mount point is displayed.
5. Select a realm and click the **Edit** button. The Edit Realm wizard displays.
6. Click **Next** to move to the Realm Objects page where you can click **Remove** to delete objects from the realm.
7. Click **Done**.

Deleting a Realm

You can delete a realm from an Oracle ACFS file system. After a realm is deleted, access to all objects that were part of the realm is reverted to the state prior to their addition to the realm. These objects are not subjected to security and encryption that were enabled on the realm.

To delete a realm, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see "[Accessing the Oracle Automatic Storage Management Home Page](#)".

2. Click the **Mount Point** that contains the realm you want to delete. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the Security section, click **Realms**. The list of realms in the mount point is displayed.
5. Select the realm you want to delete and click **Delete**.

Viewing Realms

To view realms, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see "[Accessing the Oracle Automatic Storage Management Home Page](#)".

2. Click the **Mount Point** that contains the realms you want to view. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. In the **Security** section, click **Realms**. The list of realms in the file system is displayed as shown in [Figure 10](#).

Figure 10 Oracle ACFS Security Realms Page

ASM Cluster File System: /acfsmounts/acfs1

General Snapshots **Security/Encryption**

Security

- Configuration
- Rules (7)
- Rulesets (6)
- Realms (5)**

Encryption

- Configuration

Realms

ACFS Security realms provide a capability to classify file system objects into functional groups to provide fine-grained access control to data stored in these objects. The access requests to these objects will be subjected to authorization based on the command rules and rulesets associated with the realm, once security is enabled on it.

Search Realm Name

Realm Name	Realm Description	OS Users	OS Groups	Security	Encryption
SYSTEM_SecurityMetada			sysSecAdminGrp	✓	✗
SYSTEM_Logs			sysSecAdminGrp	✓	✗
SYSTEM_Audit			sysAuditAdminGrp	✓	✗
medHistRealm		medMaintenance	medMaintGrp	✓	✓
SYSTEM_BackupOperat			sysBackupGrp	✓	✗

✓ Enabled ✗ Disabled

Managing Encryption Features with Oracle Enterprise Manager

This section describes how to manage encryption with Oracle Enterprise Manager.

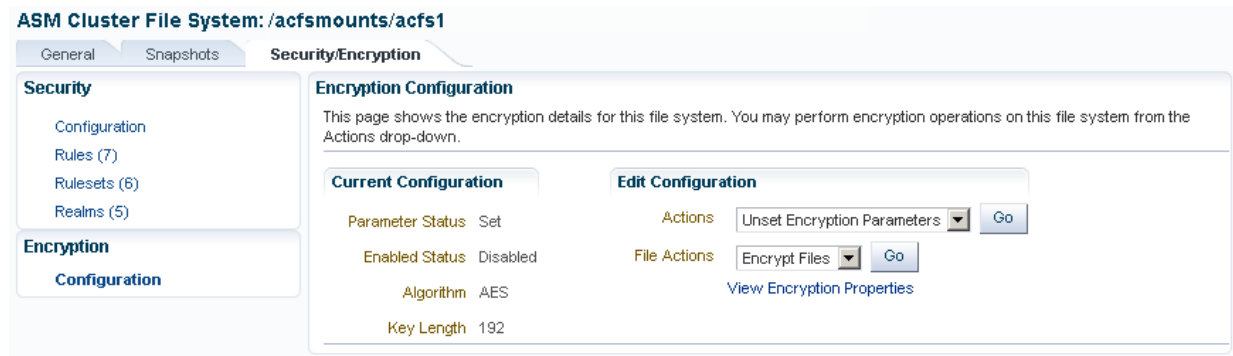
- [Initializing Oracle ACFS Encryption](#)
- [Enabling_ Disabling_ and Setting Parameters for Encryption On an Oracle ACFS](#)
- [Viewing Encryption Status](#)

For more information about Oracle ACFS encryption, refer to “[Oracle ACFS Encryption](#)”.

Initializing Oracle ACFS Encryption

To initialize Oracle ACFS encryption, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.
For information about the Oracle ASM home page and how to access that page, see “[Accessing the Oracle Automatic Storage Management Home Page](#)”.
2. Click a mount point in the list.
3. Click the **Security/Encryption** tab to display the Security and Encryption section.
4. In the **Encryption Configuration** section, you can specify various options, such as **Unset Encryption Parameters**, as shown in [Figure 11](#).
5. If Oracle ACFS encryption is not initialized in the cluster, the **Initialize Encryption** button displays. Click the button to initialize Oracle ACFS encryption. This operation needs to be performed only once in the cluster.

Figure 11 Oracle ACFS Encryption Configuration Page

Enabling, Disabling, and Setting Parameters for Encryption On an Oracle ACFS

To enable, disable, or set parameters for Oracle ACFS encryption, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.
2. Click the **Mount Point** that contains the realms you want to view. The Oracle ACFS home page is displayed for this mount point.
3. Click the **Security/Encryption** tab.
4. Click **Encryption Configuration** link to display the Encryption configuration section.

Viewing Encryption Status

To view encryption status, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Click **Show Security and Encryption** to display the Security and Encryption section.

The section displays the mount points and the security and encryption settings for each.

Managing Tagging Features with Oracle Enterprise Manager

This section describes how to manage tagging with Oracle Enterprise Manager.

- [Adding a Tag in Oracle ACFS](#)
- [Removing a Tag in Oracle ACFS](#)
- [Searching for Tags in Oracle ACFS](#)

For more information about Oracle ACFS tagging, refer to [“Oracle ACFS Tagging”](#).

Adding a Tag in Oracle ACFS

You can add tags to directories and files that reside in a single Oracle ACFS file system or across multiple Oracle ACFS file systems. With the tag names, you can organize your files or perform operations, such as search and replication.

To add tags for specific files or directories from the ASM Cluster File System Page, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Select the file or directory you want to tag and select **Add Tag** from the Actions menu, then click **Go**.

Enterprise Manager displays the Add Tag page.

3. Add a Tag Name (or a comma-delimited list of names) in the Tag Name box. Optionally, you can turn on the option that enables you to add tags recursively to subdirectories and files.
4. In the Directories and Files section, enter either the directory paths directly as a comma-delimited list in the **Enter Directory** box, or search for directory paths with the ASM Cluster File System by selecting **Search Directory**. You can add a directory path by clicking **Add**.
5. Click **OK** to add tags.

Removing a Tag in Oracle ACFS

You can remove tags for specific files or directories in an Oracle ACFS file system. Optionally, you can recursively apply the remove operation to all subdirectories and files.

To remove tags, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see [“Accessing the Oracle Automatic Storage Management Home Page”](#).

2. Select the file or directory from which you want to remove tags and select **Remove Tag** from the Actions menu, then click **Go**.

Enterprise Manager displays the Remove Tag page.

3. In the Tag Name box, enter the name of the tag you want to remove or specify a comma-delimited list of tag names to remove. Optionally, you can remove tags recursively from all directories and files that exist in the specified directory paths by turning on the option.
4. In the Directories and Files section, select **Enter Directory** to enter the directory paths directly as a comma-delimited list, or select **Search Directory** to search for directory paths within an Oracle ACFS file system. To add directory paths

repeatedly from different Oracle ACFS file systems, choose the file system and click **Add**.

5. Click **OK** to remove tags.

Searching for Tags in Oracle ACFS

You can search for tags from selected files and directories in an Oracle ACFS file system. Optionally, you can recursively apply this operation to all subdirectories and files. To search for tags for specific files or directories in an Oracle ACFS file system, follow these steps:

1. From the Oracle ASM home page, select the ASM Cluster File System tab to display the mount points in the cluster file system.

For information about the Oracle ASM home page and how to access that page, see "[Accessing the Oracle Automatic Storage Management Home Page](#)".

2. From the Action menu, select **Search Tags**, then click **Go**.

Enterprise Manager displays the Search Tags page.

3. In the Search Criteria section, specify a comma-delimited list of tag names in the Tag Name box. Optionally, you can search tags recursively in all directories and files by turning on the option.
4. In the Directories and Files section, select **Enter Directory** to enter the directory path as a comma-delimited list, or select **Search Directory** to choose the Oracle ACFS file system and click **Add** to add directory paths repeatedly from different Oracle ACFS file systems.
5. Click **Search**.

The results of the search appear in the Search Results table.

6. Click **Return** to navigate back to the Oracle ASM home page displaying the ASM Cluster File System tab.

Managing Oracle ACFS and Oracle ADVM With ASMCA

Oracle ASM Configuration Assistant (ASMCA) supports installing and configuring Oracle ASM instances, Oracle ASM disk groups, Oracle ASM Dynamic Volume Manager (Oracle ADVM) volumes, and Oracle Automatic Storage Management Cluster File System (Oracle ACFS) file systems. In addition, you can use the ASMCA command-line interface.

This chapter discusses the following topics:

- [ASMCA GUI Tool for Managing Oracle ACFS and Oracle ADVM](#)
- [ASMCA Command-Line Interface for Managing Oracle ACFS and Oracle ADVM](#)

The **Instances** tab functionality and some menu options of ASMCA are only available in an Oracle RAC configuration. For information about managing Oracle ASM instances and disk groups with ASMCA, refer to [Managing Oracle ASM With ASMCA](#).

ASMCA GUI Tool for Managing Oracle ACFS and Oracle ADVM

This section contains the following topics:

- [Managing Oracle ADVM Volumes with ASMCA](#)
- [Managing Oracle ACFS File Systems with ASMCA](#)
- [Managing Security and Encryption for Oracle ACFS with ASMCA](#)
- [Creating an Oracle ACFS File System for Database Use](#)

Managing Oracle ADVM Volumes with ASMCA

Note:

When creating an Oracle ADVM volume for an Oracle ACFS file system that is intended to store database files, use the ASMCMDB `volcreate` command or the SQL `ALTER DISKGROUP ADD VOLUME SQL` statement rather than the ASMCA tool to ensure that the column striping is set to 1. For information about the `volcreate` command, refer to [“volcreate”](#). For information about the `ALTER DISKGROUP ADD VOLUME` statement, refer to [“Managing Oracle ADVM Volumes in a Disk Group”](#).

Oracle ASM Configuration Assistant enables you to create or configure an Oracle ADVM volume, as shown in [Figure 1](#).

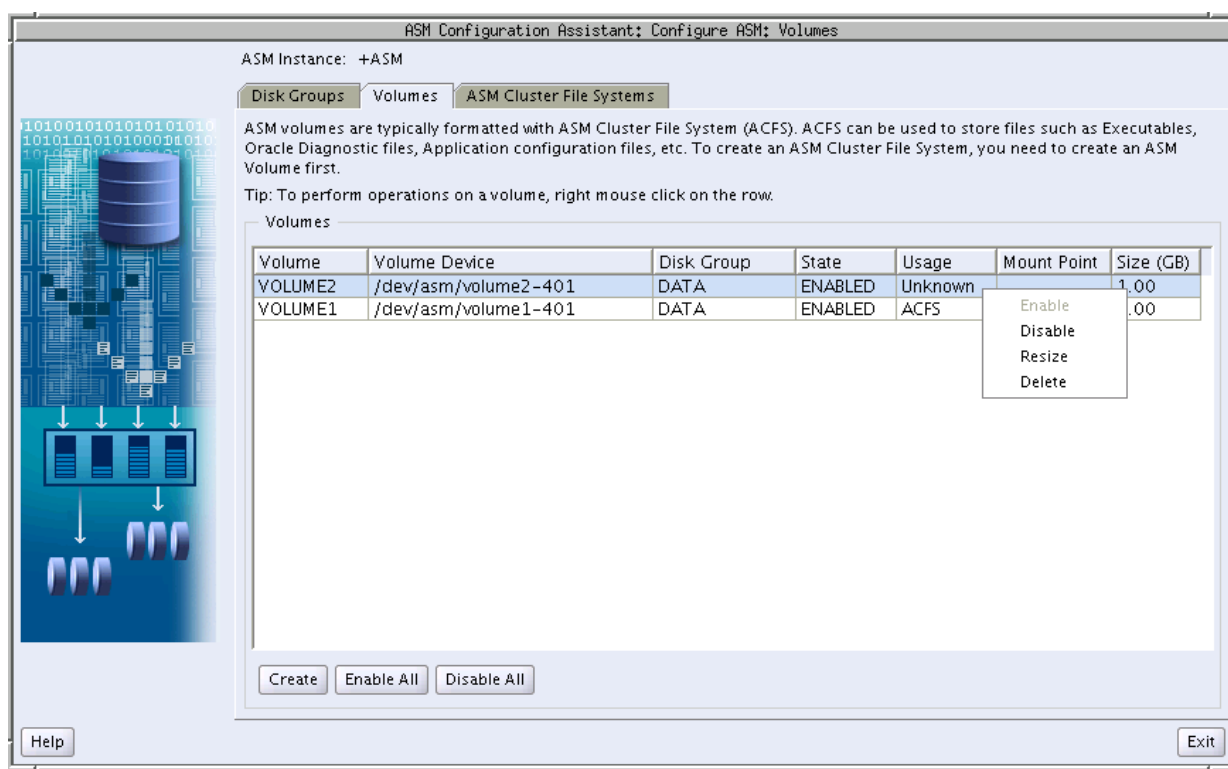
Right click a selected volume in the Oracle ASM Configuration Assistant screen to display the configuration options menu.

The menu includes options to:

- Enable disabled volumes and disable enabled volumes
- View status details
- Resize volumes that have not been mounted on an Oracle ACFS file system
- Delete volumes

There are options for creating a volume, enabling all volumes, and disabling all volumes.

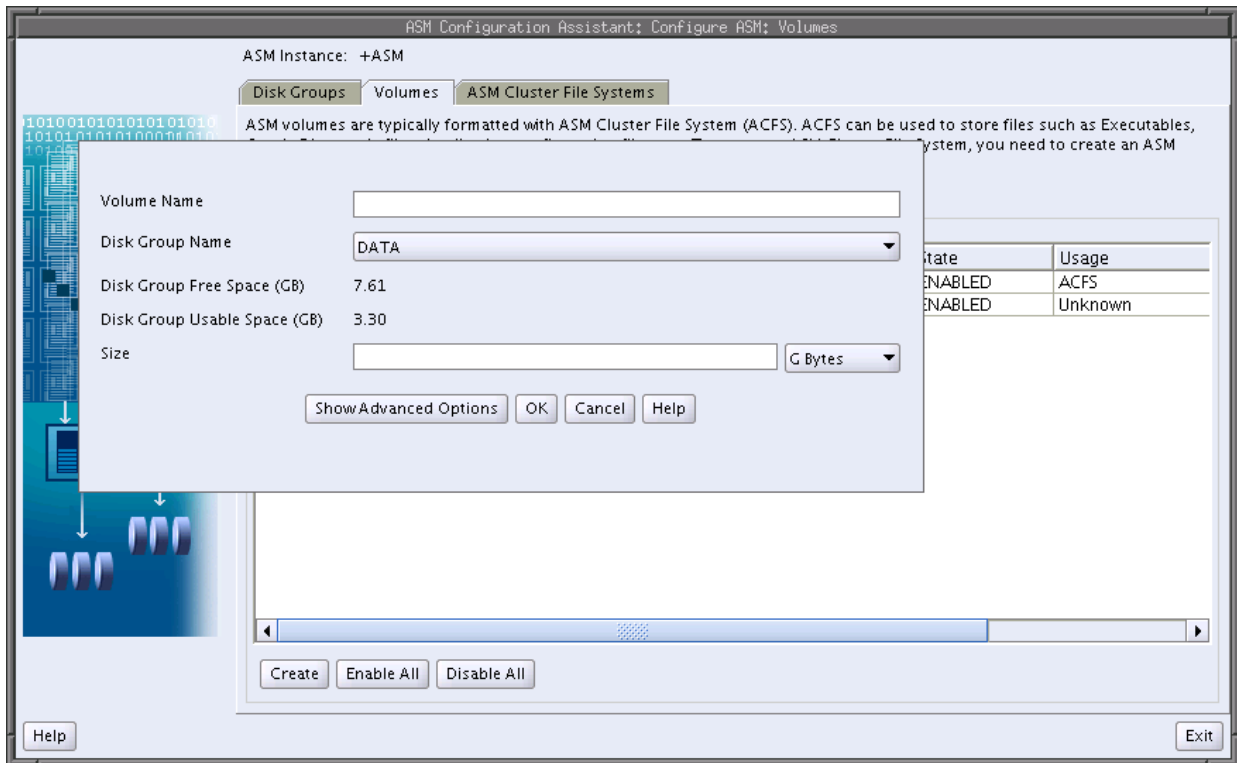
Figure 1 Oracle ASM Configuration Assistant Configure ASM Volumes Page



Click **Create** to display the dialog for creating a volume. You must provide a unique volume name for the existing Oracle ASM disk group that you select from the list of disk groups. You must also specify the size for the volume. You can optionally choose to display advanced options for creating a volume which enables you to specify the redundancy level and striping characteristics. For information about the advanced options when creating a volume, refer to “[volcreate](#)”.

The compatibility parameters `COMPATIBLE.ASM` and `COMPATIBLE.ADVM` must be set to 11.2 or higher for the disk group to contain an Oracle ADVM volume. To use Oracle ACFS encryption, replication, security, or tagging, the disk group on which the volume is created for the file system must have compatibility attributes for ASM and ADVM set to 11.2.0.2 or higher. See “[Disk Group Compatibility Attributes](#)”.

Before creating an Oracle ADVM volume on AIX, ensure that the necessary user authorizations have been created. For information, refer to “[Oracle ACFS Command-line Tools for the AIX Environment](#)”.

Figure 2 Oracle ASM Configuration Assistant Create an ASM Volume Page

For information about creating a volume with the `ASMCMD volcreate` command, refer to [Managing Oracle ADVM with ASMCMD](#). For an overview of Oracle ACFS, see [Introducing Oracle ACFS and Oracle ADVM](#).

Managing Oracle ACFS File Systems with ASMCA

Oracle ASM Configuration Assistant enables you to create or configure an Oracle ACFS file system, as shown in [Figure 3](#).

To configure an existing file system, right click a selected file system in the Oracle ASM Configuration Assistant screen to display the configuration options menu.

The menu includes options to:

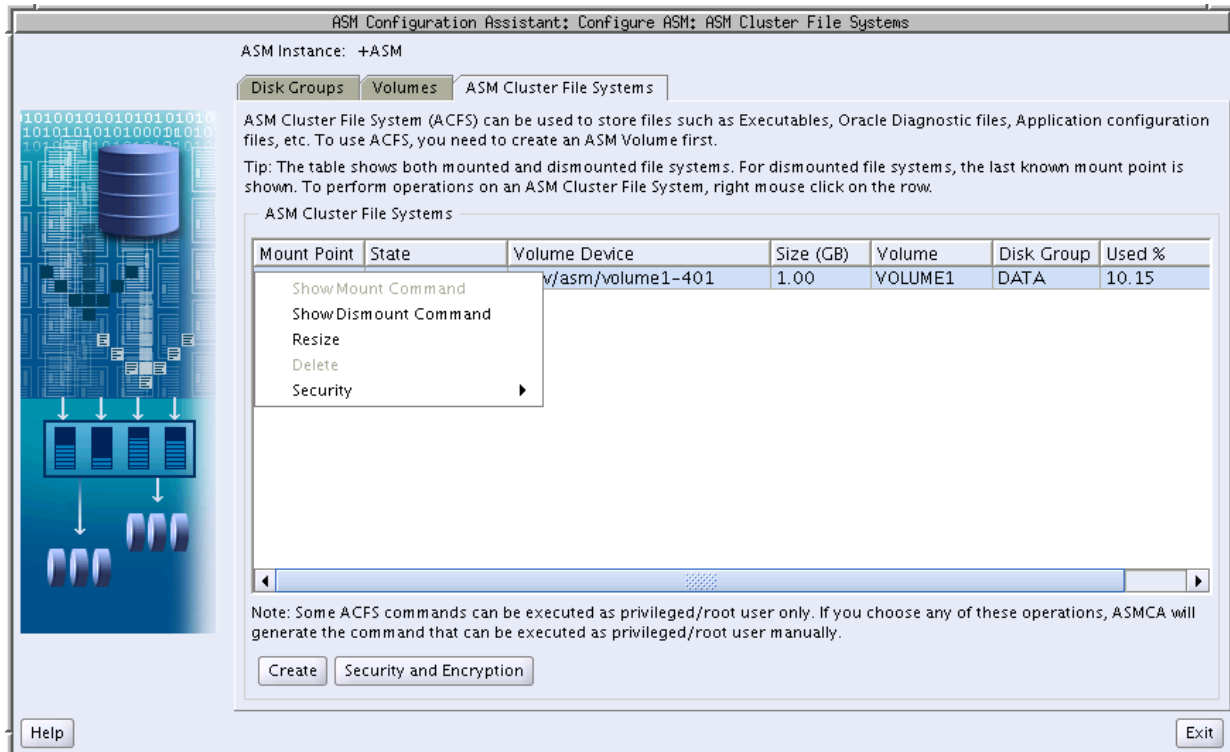
- View status details
- Mount and dismount the file system
- Resize the file system
- Delete the file system
- Display the security commands

Some commands require root privileges, such as mounting a file system. ASMCA generates the command for you to run manually as `root`.

When creating Oracle ACFS file systems on Windows, run ASMCA as a Windows domain user who is also an administrator of the computer.

There are buttons for Create, Mount All, Dismount All, and Security and Encryption commands.

Figure 3 Oracle ASM Configuration Assistant Configure Oracle ACFS Page

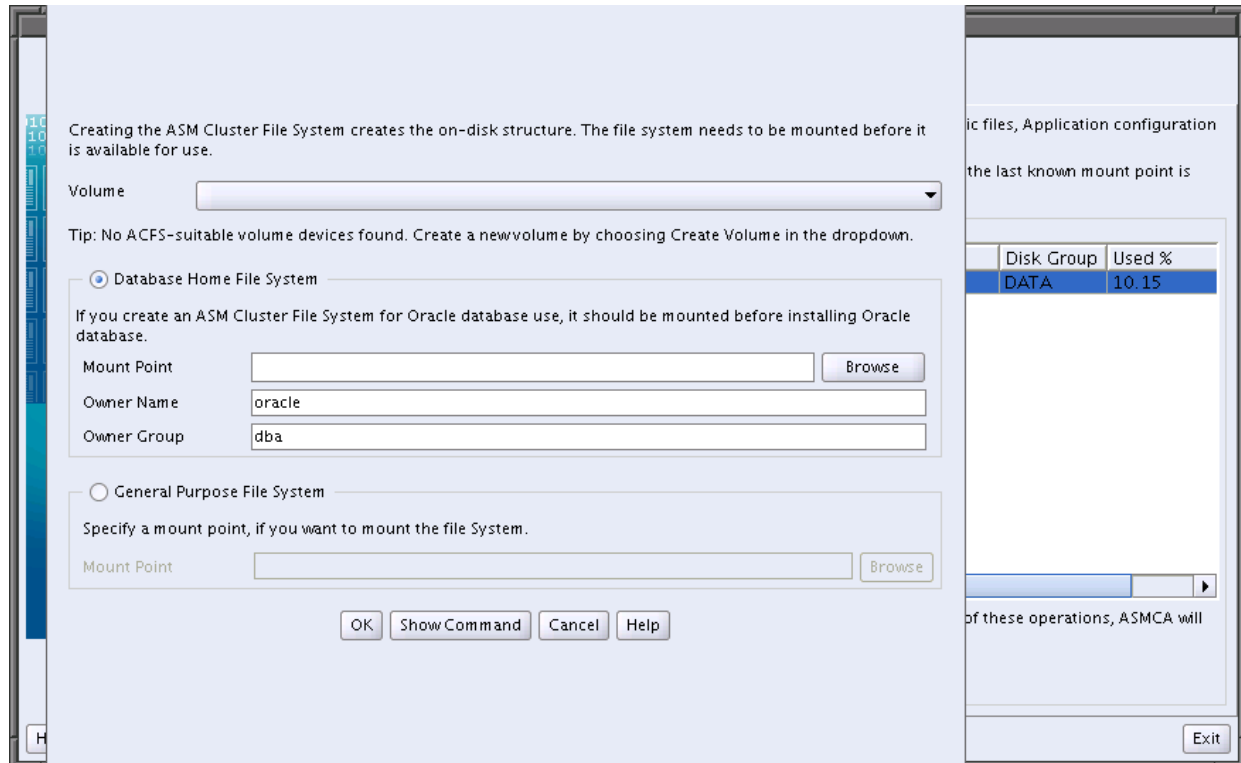


Oracle ASM Configuration Assistant enables you to create an Oracle ACFS file system, as shown in [Figure 3](#).

Select **Create**, then select the type of Oracle ACFS file system you want to create and an existing Oracle ADVM volume from the lists. Specify the mount point field; the mount point must be an existing directory. The file system must be mounted to make it available. You can choose to enable the **Auto Mount** option. You can also provide a description of the file system in the **Description** field.

The mount command must be manually run as root or the Windows Administrator at an operating system prompt. For information about mounting an Oracle ACFS file system, see “[mount](#)” for Linux or “[acfsmountvol](#)” for Windows.

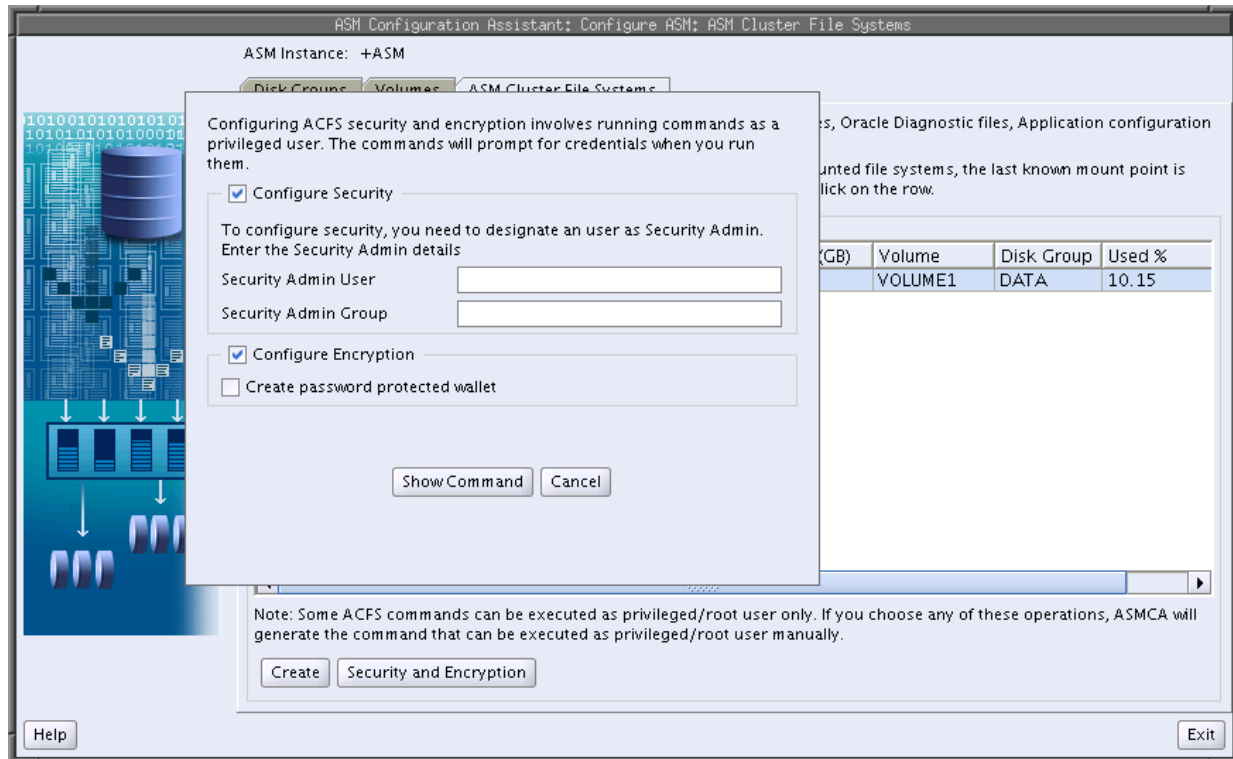
You can choose to create an Oracle ACFS file system for an Oracle Database. For more information about creating a file system for a database home, see “[Creating an Oracle ACFS File System for Database Use](#)”.

Figure 4 Oracle ASM Configuration Assistant Create Oracle ACFS Dialog

For information about Oracle ACFS, see [Introducing Oracle ACFS and Oracle ADVM](#). For a summary of the basic steps for creating an Oracle ACFS file system, see “[Basic Steps to Manage Oracle ACFS Systems](#)”.

Managing Security and Encryption for Oracle ACFS with ASMCA

Oracle ASM Configuration Assistant enables you to configure security and encryption for an Oracle ACFS file system, as shown in [Figure 5](#).

Figure 5 Oracle ASM Configuration Assistant Configure Security and Encryption Dialog

You must initialize the security system as the first step in configuring security for an Oracle ACFS file system. You must also initialize the encryption system as the first step in encrypting an Oracle ACFS file system. You do not have to use both Oracle ACFS security and encryption on the same file system. If you decide to use both security and encryption, then encryption must be initialized and set before enabling encryption on a security realm.

In the dialog shown in [Figure 5](#), enter the information to specify the security administrator and the operating system group of the security administrator. You can choose to create a password protected wallet. After you complete the entry fields in the dialog, click **Show Command** to display the commands you must run as a root or Administrator user at an operating system prompt. For example:

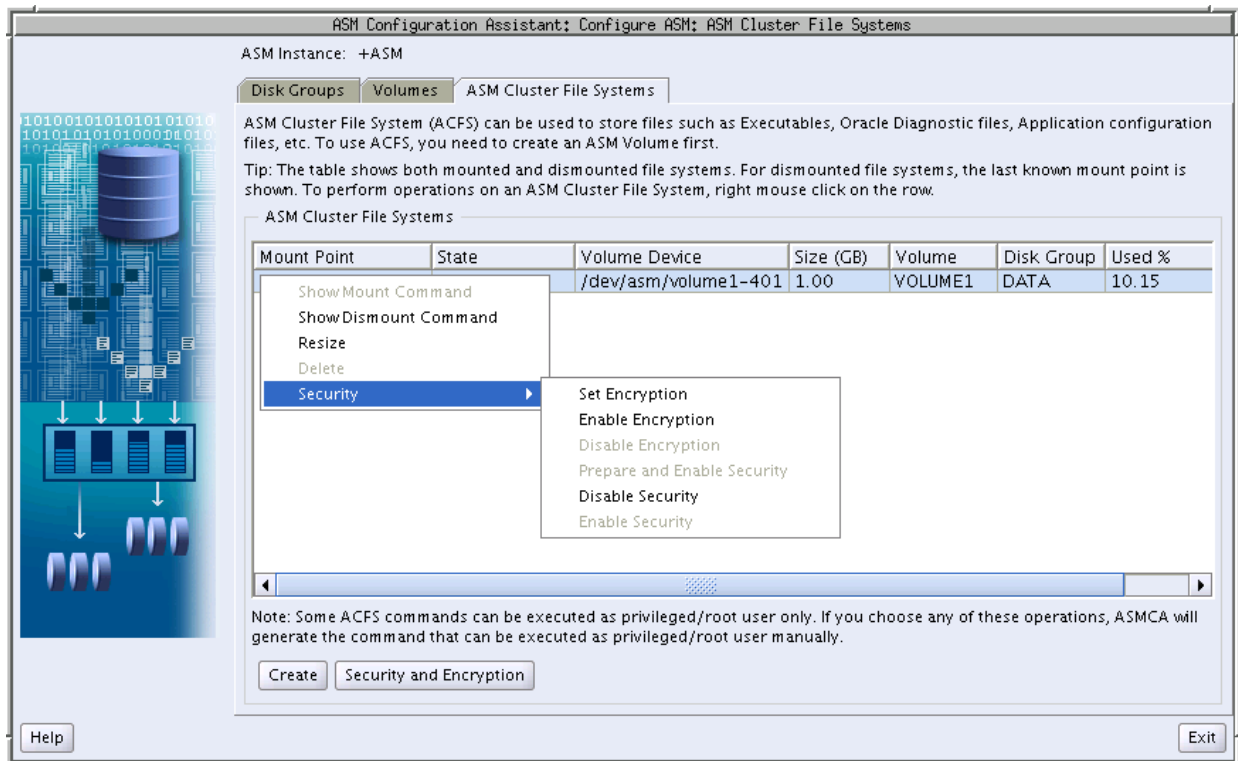
```
# /sbin/acfsutil sec init -u grid -g asmadmin
# /sbin/acfsutil encr init
```

For information about the `acfsutil sec init` and `acfsutil encr init` commands, refer to "[acfsutil sec init](#)" and "[acfsutil encr init](#)".

After security has been initialized, you can use the menu options to manage security and encryption for an Oracle ACFS file system, as shown in [Figure 6](#).

The menu includes options to:

- Set encryption
- Enable and disable encryption
- Prepare and enable security
- Enable and disable security

Figure 6 Oracle ASM Configuration Assistant Oracle ACFS Security Menu Options


For information about Oracle ACFS security, see [“Oracle ACFS Security”](#). For a summary of the basic steps for setting up security on an Oracle ACFS file system, see [“Securing Oracle ACFS File Systems”](#).

For information about Oracle ACFS encryption, see [“Oracle ACFS Encryption”](#). For a summary of the basic steps for setting up encryption on an Oracle ACFS file system, see [“Encrypting Oracle ACFS File Systems”](#).

For information about the `acfsutil encr` and `acfsutil sec` commands, see [“Oracle ACFS Command-Line Utilities”](#).

Creating an Oracle ACFS File System for Database Use

To create an Oracle ACFS file system for database use, you can select the **Create ACFS for Database Use** from the disk group configuration options menu, as shown in [Figure 4](#). A dialog displays as shown in [Figure 7](#).

Note:

When creating an Oracle ADVM volume for an Oracle ACFS file system that is intended to store database files, use the `ASMCMD volcreate` command or the SQL `ALTER DISKGROUP ADD VOLUME SQL` statement rather than the ASMCA tool to ensure that the column striping is set to 1. For information about the `volcreate` command, refer to [“volcreate”](#). For information about the `ALTER DISKGROUP ADD VOLUME` statement, refer to [“Managing Oracle ADVM Volumes in a Disk Group”](#).

In this dialog, you must enter:

- Database Home Volume Name

This is the name of the Oracle ADVM volume you want to create. For information about Oracle ADVM volumes, refer to [“Overview of Oracle ASM Dynamic Volume Manager”](#) and [“volcreate”](#).

- Database Home Mount Point

This is the mount point for the file system where you want to install the database home. The file system that contains the database home should not be located under the Oracle Grid Infrastructure base (ORACLE_BASE for grid) directory. For information about mount points and database homes, see [“About Oracle ACFS and Oracle Database Homes”](#).

- Database Home Size in gigabytes (GB)

The default is 7 GB and the minimum recommended size.

- Database Home Owner Name

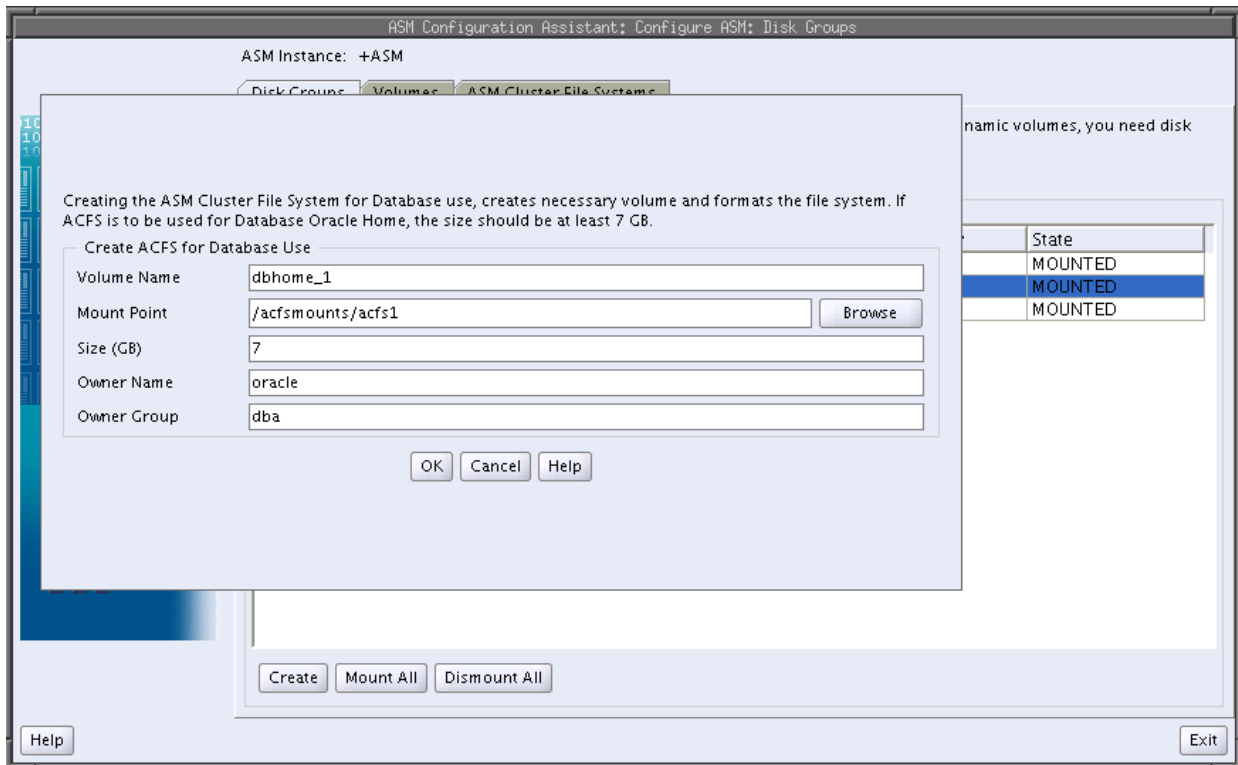
This is the operating system name of the user that installs the database and owns the software in the database home.

- Database Home Owner Group

This is the operating system group of the owner of the database home.

The mount point must be an existing directory. The file system must be mounted to make it available. The mount command must be manually run as `root` or the Windows Administrator at an operating system prompt. For information about mounting an Oracle ACFS file system, see [“mount”](#) for Linux or [“acfsmountvol”](#) for Windows.

For information on the mount registry, see [“About the Oracle ACFS Mount Registry”](#).

Figure 7 Oracle ASM Configuration Assistant Create Oracle ACFS for Database Use Dialog


ASMCA Command-Line Interface for Managing Oracle ACFS and Oracle ADVM

The ASMCA command-line interface provides non-GUI support for configuring Oracle ASM disk groups, volumes, and Oracle ACFS.

- [ASMCA Commands for Oracle ACFS and Oracle ADVM](#)

For general information about running ASMCA command-line interface, refer to [“Running ASMCA Command-Line”](#).

ASMCA Commands for Oracle ACFS and Oracle ADVM

This section describes the commands that can be run with ASMCA command-line.

- [Create a Volume](#)
- [Create an Oracle ACFS File System](#)

Run ASMCA commands as a Windows domain user.

Create a Volume

`-createVolume` creates Oracle ADVM volumes.

Syntax

```
asmca -silent
      -createVolume
        { -volumeName volume_name
          -volumeDiskGroup diskgroup
```

```

        -volumeSizeGB size_GB
    [ -volumeRedundancy { INHERIT | HIGH | NORMAL | EXTERNAL } ] ... }
[-sysAsmPassword sysasm_password ]
    
```

[Table 1](#) contains the options available with the `-createVolume` command.

Table 1 Options for the `-createVolume` command

Option	Description
<code>-volumeName <i>volume_name</i></code>	Specifies the name of the volume to create.
<code>-volumeDiskGroup <i>diskgroup</i></code>	Specifies the name of the disk group where you want to create the volume.
<code>-volumeSizeGB <i>size_GB</i></code>	Specifies the size of the volume in Gigabytes.
<code>-volumeRedundancy { INHERIT HIGH NORMAL EXTERNAL }</code>	Specifies the redundancy setting for the volume.

For additional options that are common to multiple commands, see [Table 1](#).

Examples

To create an Oracle ADVM volume:

Example 1 Using `asmca -silent -createVolume`

```

$ asmca -silent
  -createVolume
    -volumeName volume1
    -volumeDiskGroup mynewdg
    -volumeSizeGB 1
    
```

Volume *volume1* created successfully.

Create an Oracle ACFS File System

`-createACFS` creates an Oracle Automatic Storage Management Cluster File System (Oracle ACFS).

This command does not mount the Oracle ACFS file system. For information about mounting an Oracle ACFS file system, see “[mount](#)” for Linux environments and “[acfsmountvol](#)” for Windows environments.

Syntax

```

asmca -silent
  -createACFS
    { -acfsVolumeDevice volume_device }
    { -acfsMountPoint mount_path }
    [-acfsUserName acfs_username ]
    [-acfsUserGroup acfs_usergroup ]
    [-sysAsmPassword sysasm_password ]
    
```

[Table 2](#) contains the options available with the `-createACFS` command.

Table 2 Options for the `-createACFS` command

Option	Description
<code>-acfsVolumeDevice <i>volume_device</i></code>	Specifies the name of the Oracle ADVM volume device.

Option	Description
<code>-acfsMountPoint <i>mount_path</i></code>	Specifies an existing path to be used as the mount point. This is required in an Oracle RAC environment.
<code>-acfsUserName <i>acfs_username</i></code>	Specifies the Oracle ACFS user name.
<code>-acfsUserGroup <i>acfs_usergroup</i></code>	Specifies the Oracle ACFS group name.

For additional options that are common to multiple commands, see [Table 1](#) .

Examples

To create an Oracle ACFS file system:

Example 2 Using `asmca -silent -createACFS`

```
$ asmca -silent
  -createACFS
    -acfsVolumeDevice /dev/asm/volume1-457
    -acfsMountPoint /acfsmounts/acfs1
```


Managing Oracle ADVM with ASMCMD

This chapter describes the Oracle Automatic Storage Management (Oracle ASM) Command-Line Utility (ASMCMD) volume management commands.

- [ASMCMD Volume Management Commands](#)

For information about Oracle ASM Dynamic Volume Manager (Oracle ADVM), refer to “[Overview of Oracle ASM Dynamic Volume Manager](#)”. For information about using SQL statements to manage Oracle ADVM volumes, refer to “[Managing Oracle ADVM Volumes in a Disk Group](#)”.

For information about using ASMCMD, refer to “[About ASMCMD](#)”.

ASMCMD Volume Management Commands

[page 15-1](#) provides a summary of the Oracle ADVM volume management commands. To successfully run these commands, the local Oracle ASM instance must be running and the disk group required by this command must have been created and mounted in the Oracle ASM instance.

Command	Description
volcreate	Creates an Oracle ADVM volume in the specified disk group.
voldelete	Deletes an Oracle ADVM volume.
voldisable	Disables Oracle ADVM volumes in mounted disk groups.
volenable	Enables Oracle ADVM volumes in mounted disk groups.
volinfo	Displays information about Oracle ADVM volumes.
volresize	Resizes an Oracle ADVM volume.
volset	Sets attributes of an Oracle ADVM volume in mounted disk groups.
volstat	Reports volume I/O statistics.

volcreate

Purpose

Creates an Oracle ADVM volume in the specified disk group.

Syntax and Description

```
volcreate -G diskgroup -s size
      [ --column number ] [ --width stripe_width ]
      [--redundancy {high|mirror|unprotected}]
      [--primary {hot|cold}] [--secondary {hot|cold}] volume
```

Table 2 describes the options for the `volcreate` command.

Table 2 Options for the `volcreate` command

Option	Description
<code>-G diskgroup</code>	Name of the disk group containing the volume.
<code>-s size</code>	Size of the volume to be created in units of K, M, G, or T. The value must be a positive integer. The unit designation must be appended to the number specified. A space is not allowed between the number and the unit designation. For example: 200M or 20G
<code>--column number</code>	Number of columns in a stripe set. Values range from 1 to 8. The default value is 8.
<code>--width stripe</code>	Stripe width of a volume in units of K or M. The value can range from 4 KB to 1 MB, at power-of-two intervals. The default is 1M.
<code>--redundancy {high mirror unprotected}</code>	Redundancy of the Oracle ADVM volume which can be only specified for normal redundancy disk groups. If redundancy is not specified, the setting defaults to the redundancy level of the disk group and this is the recommended setting. The range of values is as follows: <code>unprotected</code> for non-mirrored redundancy, <code>mirror</code> for double-mirrored redundancy, or <code>high</code> for triple-mirrored redundancy.
<code>--primary {hot cold}</code>	Intelligent Data Placement specification for primary extents, either <code>hot</code> or <code>cold</code> region.
<code>--secondary {hot cold}</code>	Intelligent Data Placement specification for secondary extents, either <code>hot</code> or <code>cold</code> region.
<code>volume</code>	Name of the volume. Only alphanumeric characters are allowed; hyphens are not allowed. The first character must be alphabetic.

Warning:

Specifying `--redundancy unprotected` means that Oracle ASM mirroring is not available for data recovery with the Oracle ADVM volume. The redundancy setting (`normal`) of the disk group does not provide mirroring for an unprotected Oracle ADVM volume. The `unprotected` configuration is not recommended for production environments as intermittent storage access failures can result in the loss of data. Backups are strongly recommended.

When creating an Oracle ADVM volume, a volume device name is created with a unique Oracle ADVM persistent disk group number that is concatenated to the end of the volume name. The unique number can be one to three digits.

On Linux, the volume device name is in the format `volume_name-nnn`, such as `volume1-123`. On Windows the volume device name is in the format `asm-volume_name-nnn`, such as `asm-volume1-123`. For information on mounting the volume device file, see “[Creating an Oracle ACFS File System](#)”.

On Linux platforms, the volume name must be less than or equal to eleven alphanumeric characters, starting with an alphabetic character. On AIX platforms, the volume name must be less than or equal to twenty three alphanumeric characters,

starting with an alphabetic character. On Windows and Solaris platforms, the volume name must be less than or equal to thirty alphanumeric characters, starting with an alphabetic character.

You can determine the volume device name with the `volinfo` command, described in [“volinfo”](#).

If the `--column` option is set to 1, then striping is disabled and the stripe width equals the volume extent size. The volume extent size is 8 MB if the disk group allocation unit (AU) is less than or equal to 8 MB. If the AU size is greater than 8 MB, then the Oracle ADVM volume extent size is equivalent to the disk group AU size. For information about Oracle ADVM limits, refer to [“Limits of Oracle ADVM”](#). Setting the `--column` option to 8 (the default) is recommended to achieve optimal performance with database data files and other files.

A successful volume creation automatically enables the volume device.

The volume device file functions as any other disk or logical volume to mount file systems or for applications to use directly.

When creating an accelerator volume, create the volume on a disk group with storage that is significantly faster than the primary volume's storage. For more information about the accelerator volume, refer to [“mkfs”](#).

For information about redundancy settings, see [“Mirroring, Redundancy, and Failure Group Options”](#). For information about hot and cold disk regions, see [“Intelligent Data Placement”](#).

Before creating an Oracle ADVM volume on AIX, ensure that the necessary user authorizations have been created. For information, refer to [“Oracle ACFS Command-line Tools for the AIX Environment”](#).

Examples

The following is an example of the `volcreate` command that creates `volume1` in the data disk group with the size set to 10 gigabytes.

Example 1 Using the ASMCMD `volcreate` command

```
ASMCMD [+] > volcreate -G data -s 10G --width 1M --column 8 volume1
```

```
ASMCMD [+] > volinfo -G data volume1
```

```
Diskgroup Name: DATA

Volume Name: VOLUME1
Volume Device: /dev/asm/volume1-123
State: ENABLED
Size (MB): 10240
Resize Unit (MB): 64
Redundancy: MIRROR
Stripe Columns: 8
Stripe Width (K): 1024
Usage:
Mountpath:
```

voldelete

Purpose

Deletes an Oracle ADVM volume.

Syntax and Description

```
voldelete -G diskgroup volume
```

[Table 3](#) describes the options for the `voldelete` command.

Table 3 Options for the `voldelete` command

Option	Description
<code>-G <i>diskgroup</i></code>	Name of the disk group containing the volume.
<code><i>volume</i></code>	Name of the volume.

To successfully run this command, the local Oracle ASM instance must be running and the disk group required by this command must be mounted in the Oracle ASM instance. Before deleting a volume, you must ensure that there are no active file systems associated with the volume.

Examples

The following is an example of the `voldelete` command that deletes `volume1` from the data disk group.

Example 2 Using the ASMCMD `voldelete` command

```
ASMCMD [+] > voldelete -G data volume1
```

voldisable**Purpose**

Disables Oracle ADVM volumes in mounted disk groups and removes the volume device on the local node.

Syntax and Description

```
voldisable { --all | { -G diskgroup { -a | volume } } }
```

[Table 4](#) describes the options for the `voldisable` command.

Table 4 Options for the `voldisable` command

Option	Description
<code>-all</code>	Specifies all volumes within all disk groups.
<code>-G <i>diskgroup</i></code>	Name of the disk group containing the volume.
<code>-a</code>	Specifies all volumes within the specified disk group.
<code><i>volume</i></code>	Name of the volume.

You can disable volumes before shutting down an Oracle ASM instance or dismounting a disk group to verify that the operations can be accomplished normally without including a force option due to open volume files. Disabling a volume also prevents any subsequent opens on the volume or device file because it no longer exists.

Before disabling a volume, you must ensure that there are no active file systems associated with the volume. You must first dismount the Oracle ACFS file system before disabling the volume. See [“Dismounting an Oracle ACFS File System”](#).

You can delete a volume without first disabling the volume.

Examples

The following is an example of the `voldisable` command that disables `volume1` in the `data` disk group.

Example 3 Using the ASMCMD voldisable command

```
ASMCMD [+] > voldisable -G data volume1
```

volenable

Purpose

Enables Oracle ADVM volumes in mounted disk groups.

Syntax and Description

```
volenable { --all | { -G diskgroup { -a | volume } } }
```

[Table 5](#) describes the options for the `volenable` command.

Table 5 Options for the volenable command

Option	Description
<code>-all</code>	Specifies all volumes within all disk groups.
<code>-G <i>diskgroup</i></code>	Name of the disk group containing the volume.
<code>-a</code>	Specifies all volumes within the specified disk group.
<code><i>volume</i></code>	Name of the volume.

A volume is enabled when it is created.

Examples

The following is an example of the `volenable` command that enables `volume1` in the `data` disk group.

Example 4 Using the ASMCMD volenable command

```
ASMCMD [+] > volenable -G data volume1
```

volinfo

Purpose

Displays information about Oracle ADVM volumes.

Syntax and Description

```
volinfo { --all | { -G diskgroup { -a | volume } } }  
volinfo {--show_diskgroup | --show_volume} volumedevice
```

[Table 6](#) describes the options for the `volinfo` command.

Table 6 Options for the volinfo command

Option	Description
-all	Specifies all volumes within all disk groups.
-G <i>diskgroup</i>	Name of the disk group containing the volume.
-a	Specifies all volumes within the specified disk group.
<i>volume</i>	Name of the volume.
--show_diskgroup	Returns only the disk group name. A volume device name is required.
--show_volume	Returns only the volume name. A volume device name is required.
<i>volumedevic</i>	Name of the volume device.

Examples

The first example displays information about the `volume1` volume in the `data` disk group. This example was produced in a Linux environment. The second example displays information about the `volume1` volume in the `data` disk group and was produced in a Windows environment.

The `Mountpath` field contains the path where the volume is currently mounted or where the volume was last mounted.

Example 5 Using the ASMCMD volinfo command

```
ASMCMD [+] > volinfo -G data volume1
Diskgroup Name: DATA
  Volume Name: VOLUME1
  Volume Device: /dev/asm/volume1-123
  State: ENABLED
  Size (MB): 10240
  Resize Unit (MB): 64
  Redundancy: MIRROR
  Stripe Columns: 8
  Stripe Width (K): 1024
  Usage: ACFS
  Mountpath: /acfsmounts/acfs1

ASMCMD [+] > volinfo -G data -a
Diskgroup Name: DATA
  Volume Name: VOLUME1
  Volume Device: \\.\asm-volume1-311
  State: ENABLED
  Size (MB): 10240
  Resize Unit (MB): 64
  Redundancy: MIRROR
  Stripe Columns: 8
  Stripe Width (K): 1024
  Usage: ACFS
  Mountpath: C:\oracle\acfsmounts\acfs1
```

volresize

Purpose

Resizes an Oracle ADVM volume.

Syntax and Description

```
volresize -G diskgroup -s size [ -f ] volume
```

Table 7 describes the options for the `volresize` command.

Table 7 Options for the `volresize` command

Option	Description
<code>-G <i>diskgroup</i></code>	Name of the disk group containing the volume.
<code>-f</code>	Forces the shrinking of a volume that is not an Oracle ACFS volume and suppresses any warning message.
<i>volume</i>	Name of the volume.
<code>-s <i>size</i></code>	New size of the volume in units of K, M, G, or T.

If the volume is mounted on a non-Oracle ACFS file system, then dismount the file system first before resizing. If the new size is smaller than current, you are warned of possible data corruption. Unless the `-f` (force) option is specified, you are prompted whether to continue with the operation.

If there is an Oracle ACFS file system on the volume, then you cannot resize the volume with the `volresize` command. You must use the `acfsutil size` command, which also resizes the volume and file system. For information, see “[acfsutil size](#)”.

Examples

The following is an example of the `volresize` command that resizes `volume1` in the data disk group to 20 gigabytes.

Example 6 Using the ASMCMD `volresize` command

```
ASMCMD [+] > volresize -G data -s 20G volume1
```

volset

Purpose

Sets attributes of an Oracle ADVM volume in mounted disk groups.

Syntax and Description

```
volset -G diskgroup [ --usagestring string ]
      [--mountpath mount_path ]
      [--primary {hot|cold}] [--secondary {hot|cold}] volume
```

Table 8 describes the options for the `volset` command.

Table 8 Options for the `volset` command

Option	Description
<code>-G <i>diskgroup</i></code>	Name of the disk group containing the volume.
<code>--usagestring <i>string</i></code>	Optional usage string to tag a volume which can be up to 30 characters. This string is set to ACFS when the volume is attached to an Oracle ACFS file system and should not be changed.

Option	Description
<code>--mountpath <i>mount_path</i></code>	Optional string to tag a volume with its mount path string which can be up to 1024 characters. This string is set when the file system is mounted and should not be changed.
<code>--primary {hot cold}</code>	Intelligent Data Placement specification for primary extents, either <code>hot</code> or <code>cold</code> region.
<code>--secondary {hot cold}</code>	Intelligent Data Placement specification for secondary extents, either <code>hot</code> or <code>cold</code> region.
<i>volume</i>	Name of the volume.

When running the `mkfs` command to create a file system, the `usage` field is set to `ACFS` and `mountpath` field is reset to an empty string if it has been set. The `usage` field should remain at `ACFS`.

When running the `mount` command to mount a file system, the `mountpath` field is set to the mount path value to identify the mount point for the file system. After the value is set by the `mount` command, the `mountpath` field should not be updated.

Examples

The following is an example of a `volset` command that sets the usage string for a volume that is not associated with a file system.

Example 7 Using the ASMCMD volset command

```
ASMCMD [+] > volset -G data --usagestring 'no file system created' volume1
```

volstat

Purpose

Reports I/O statistics for Oracle ADVM volumes.

Syntax and Description

```
volstat [-G diskgroup] [volume]
```

[Table 9](#) describes the options for the `volstat` command.

Table 9 Options for the volstat command

Option	Description
<code>-G <i>diskgroup</i></code>	Name of the mounted disk group containing the volume.
<i>volume</i>	Name of the volume.

The following apply when using the `volstat` command.

- If the disk group is not specified and the volume name is specified, all mounted disk groups are searched for the specified volume name.
- If the disk group name is specified and the volume name is omitted, all volumes are displayed for the named disk group.
- If both the disk group name and the volume name are omitted, all volumes on all disk groups are displayed.

Examples

The following is an example of the `volstat` command that displays information about volumes in the data disk group.

Example 8 *Using the ASMCMD volstat command*

```
ASMCMD [+] > volstat -G data
DISKGROUP NUMBER / NAME: 1 / DATA
-----
VOLUME_NAME
  READS          BYTES_READ    READ_TIME     READ_ERRS
  WRITES         BYTES_WRITTEN WRITE_TIME     WRITE_ERRS
-----
VOLUME1
  10085          2290573312   22923         0
  1382          5309440      1482          0
```

Managing Oracle ACFS with Command-Line Tools

Command-line tools for managing and implementing Oracle Automatic Storage Management Cluster File System (Oracle ACFS), include the following:

- [Basic Steps to Manage Oracle ACFS Systems](#)
- [Oracle ACFS Command-line Tools for Linux Environments](#)
- [Oracle ACFS Command-line Tools for the Solaris Environment](#)
- [Oracle ACFS Command-line Tools for the AIX Environment](#)
- [Oracle ACFS Command-line Tools for Windows Environments](#)
- [Oracle ACFS Command-Line Tools for Tagging](#)
- [Oracle ACFS Command-Line Tools for Replication](#)
- [Oracle ACFS Command-Line Tools for Auditing](#)
- [Oracle ACFS Command-Line Tools for Security](#)
- [Oracle ACFS Command-Line Tools for Encryption](#)
- [Oracle ACFS Command-Line Utilities](#)

Note:

Oracle ACFS encryption, replication, security, and tagging are available starting with Oracle Automatic Storage Management (Oracle ASM) 11g Release 2 (11.2.0.2) on Linux and Oracle ASM 11g Release 2 (11.2.0.3) on Windows.

Basic Steps to Manage Oracle ACFS Systems

This section provides an outline of the basic steps when managing Oracle ACFS file systems using command-line utilities.

The examples in this section show operating system commands that are run in a Linux environment system. ASMCMD commands manage the Oracle ADVM volumes, but you can also use SQL*Plus and Oracle ASM Configuration Assistant (ASMCA) to manage volumes.

This section contains these topics:

- [Creating an Oracle ACFS File System](#)

- [Accessing an Oracle ACFS File System on a Different Node in the Cluster](#)
- [Managing Oracle ACFS Snapshots](#)
- [Securing Oracle ACFS File Systems](#)
- [Encrypting Oracle ACFS File Systems](#)
- [Tagging Oracle ACFS File Systems](#)
- [Replicating Oracle ACFS File Systems](#)
- [Deregistering_ Dismounting_ and Disabling Volumes and Oracle ACFS File Systems](#)
- [Removing an Oracle ACFS File System and a Volume](#)

Creating an Oracle ACFS File System

To create and verify a file system, perform the following steps:

1. Create an Oracle ADVM volume in a mounted disk group with the ASMCMD `volcreate` command.

The compatibility parameters `COMPATIBLE.ASM` and `COMPATIBLE.ADVM` must be set to 11.2 or higher for the disk group to contain an Oracle ADVM volume. To use Oracle ACFS encryption, replication, security, or tagging, the disk group on which the volume is created for the file system must have compatibility attributes for ASM and ADVM set to 11.2.0.2 or higher. See [“Disk Group Compatibility Attributes”](#).

Start ASMCMD connected to the Oracle ASM instance. You must be a user in the OSASM operating system group. See [“About Privileges for Oracle ASM”](#).

When configuring Oracle ADVM volume devices within a disk group, Oracle recommends assigning the Oracle Grid Infrastructure user and Oracle ASM administrator roles to users who have root privileges.

To create a volume:

```
ASMCMD [+] > volcreate -G data -s 10G volume1
```

When creating an Oracle ADVM volume, a volume device name is created that includes a unique Oracle ADVM persistent disk group number. The volume device file functions in the same manner as any other disk or logical volume to mount file systems or for applications to use directly.

The format of the volume name is platform-specific. For information about the syntax of the `volcreate` command, see [“ASMCMD Volume Management Commands”](#).

2. Determine the device name of the volume that was created.

You can determine the volume device name with the ASMCMD `volinfo` command or from the `VOLUME_DEVICE` column in the `V$ASM_VOLUME` view.

For example:

```
ASMCMD [+] > volinfo -G data volume1
Diskgroup Name: DATA

Volume Name: VOLUME1
Volume Device: /dev/asm/volume1-123
```

```

        State: ENABLED
    ...

SQL> SELECT volume_name, volume_device FROM V$ASM_VOLUME
       WHERE volume_name = 'VOLUME1';

VOLUME_NAME          VOLUME_DEVICE
-----
VOLUME1              /dev/asm/volume1-123

```

For information about the `volinfo` command, see [Managing Oracle ADVM with ASMCMD](#).

See Also:

Oracle Database Reference for information about the `V$ASM_VOLUME` view

3. Create a file system with the Oracle ACFS `mkfs` command.

Create a file system using an existing volume device.

For example:

```

$ /sbin/mkfs -t acfs /dev/asm/volume1-123

mkfs.acfs: version                = 11.2.0.1.0.0
mkfs.acfs: on-disk version        = 39.0
mkfs.acfs: volume                 = /dev/asm/volume1-123
mkfs.acfs: volume size            = 10737418240
mkfs.acfs: Format complete.

```

See “[mkfs](#)” (Linux environments) or “[acfsformat](#)” (Windows). The `root` privilege is not required. The ownership of the volume device file dictates who can run this command.

4. Optionally register the file system with the `acfsutil registry` command.

For example:

```

$ /sbin/acfsutil registry -a /dev/asm/volume1-123 /acfsmounts/acfs1

acfsutil registry: mount point /acfsmounts/acfs1 successfully added
to Oracle Registry

```

See “[acfsutil registry](#)”. The `root` or `asmadmin` privileges are required to modify the registry. The Windows Administrator privilege is equivalent to the `root` privilege on Linux.

Registering a file system is optional. After registering an Oracle ACFS file system in the cluster mount registry, the file system is mounted automatically on each cluster member listed in the registry entry during the next registry check action. This automatic process runs every 30 seconds and eliminates the requirement to manually mount the file system on each member of the cluster.

Registering an Oracle ACFS file system also causes the file system to be mounted automatically whenever Oracle Clusterware or the system is restarted.

Note:

In an Oracle Grid Infrastructure Clusterware configuration, you can run `srvctl add filesystem` to automount a file system; this method is required when an Oracle Database home is installed on an Oracle ACFS file system. However, that file system should not be added to the registry. For information about Server Control Utility (SRVCTL), see *Oracle Real Application Clusters Administration and Deployment Guide*.

For more information, see “[About the Oracle ACFS Mount Registry](#)”.

Note:

Oracle ACFS registration (`acfsutil registry`) is not supported in an Oracle Restart (standalone) configuration, which is a single-instance (non-clustered) environment.

5. Mount the file system with the Oracle ACFS `mount` command. You can mount a file system before or after registering the file system. If the file system has been registered, you can wait for the file system to be mounted automatically.

For example:

```
# /bin/mount -t acfs /dev/asm/volume1-123 /acfsmounts/acfs1
```

See “[mount](#)” (Linux environments) or “[acfsmountvol](#)” (Windows). The `root` privilege is required to run the `mount` command and the Windows Administrator privilege is required to run the `acfsmountvol` command.

After the file system has been mounted, ensure that the permissions are set to allow access to the file system for the appropriate users. For example:

```
# chown -R oracle:dba /acfsmounts/acfs1
```

6. Create a test file in the file system.

The user that creates the test file should be a user that is intended to access the file system. This test ensures that the appropriate user can write to the file system.

For example:

```
$ echo "Oracle ACFS File System" > /acfsmounts/acfs1/myfile
```

7. List the contents of the test file that was created in the file system.

For example:

```
$ cat /acfsmounts/acfs1/myfile
Oracle ACFS File System
```

Accessing an Oracle ACFS File System on a Different Node in the Cluster

If the node is part of a cluster, perform the following steps on node 2 to view the test file you created on node 1.

Note:

If the file system has been registered with the Oracle ACFS mount registry, you can skip steps 1 to 3.

1. Enable the volume that was previously created and enabled on node 1.

Start ASMCMD connected to the Oracle ASM instance. You must be a user in the OSASM operating system group. See [“About Privileges for Oracle ASM”](#).

For example:

```
ASMCMD [+] > volenable -G data volume1
```

See [Managing Oracle ADVM with ASMCMD](#).

2. View information about the volume that you created on node 1.

For example:

```
ASMCMD [+] > volinfo -G data volume1
```

See [Managing Oracle ADVM with ASMCMD](#).

3. Mount the file system using the Oracle ACFS mount command.

For example:

```
# /bin/mount -t acfs /dev/asm/volume1-123 /acfsmounts/acfs1
```

See [“mount”](#) (Linux environments) or [“acfsmountvol”](#) (Windows). The root privilege is required run the mount command and the Windows Administrator privilege is required to run the acfsmountvol command.

After the file system has been mounted, ensure that the permissions are set to allow access for the appropriate users.

4. List the contents of the test file you previously created on the file system.

For example:

```
$ cat /acfsmounts/acfs1/myfile
Oracle ACFS File System
```

The contents should match the file created previously on node 1.

Managing Oracle ACFS Snapshots

To create and verify a snapshot on node 1:

1. Create snapshot of the new file system created on node 1.

For example:

```
$ /sbin/acfsutil snap create mysnapshot_20090725 /acfsmounts/acfs1
```

See [“acfsutil snap create”](#).

2. Update the test file in the file system so that it is different than the snapshot.

For example:

```
$ echo "Modifying a file in Oracle ACFS File System" > /acfsmounts/acfs1/myfile
```

3. List the contents of the test file and the snapshot view of the test file.

For example:

```
$ cat /acfsmounts/acfs1/myfile
```

```
$ cat /acfsmounts/acfs1/.ACFS/snaps/mysnapshot_20090725/myfile
```

The contents of the test file and snapshot should be different. If node 1 is in a cluster, then you can perform the same list operation on node 2.

Securing Oracle ACFS File Systems

This section discusses the basic operations to manage security for an Oracle ACFS file system on Linux.

The scenario in this section shows how to use Oracle ACFS security to ensure that only the maintenance user can access medical history files during the maintenance period. Oracle ACFS encryption is also enabled on the same file system.

In this scenario, the disk group on which the volume is created for the file system has compatibility attributes for ASM and ADVM set to 11.2.0.3 or higher. For information about disk group compatibility, refer to [“Disk Group Compatibility”](#).

For the examples in this section, various operating system users, operating system groups, and directories must exist.

The basic steps to manage security are:

1. Initialize security for Oracle ACFS.

Run the `acfsutil sec init` command to configure storage for security credentials and identify an operating system user as the first security administrator and the operating system security group. The security administrator must belong to the operating system group. This command must be run before any other security command and requires root or Windows Administrator privileges to run.

The `acfsutil sec init` command is only run once to set up Oracle ACFS security for each cluster and can be run from any node in the cluster. Other security commands can also be run from any node in a cluster. Security administrators are common for all Oracle ACFS file systems in a cluster.

For example, the following command initializes security for a cluster and creates the first security administrator (`medHistAdmin1`).

```
# /sbin/acfsutil sec init -u medHistAdmin1 -g medHistAdminGrp
```

The `medHistAdmin1` security administrator must belong to the `medHistAdminGrp` operating system group. That group is identified as the security group for the security administrators.

When the root user or Windows Administrator user runs the command, the user assigns a security password to the security administrator. The first security administrator can change the password with the `acfsutil sec admin password` command. The valid password format is described in [“acfsutil sec init”](#). For information about `acfsutil sec admin password`, refer to [“acfsutil sec admin password”](#).

All `acfsutil sec` commands (other than `acfsutil sec init`) must be run by an Oracle ACFS security administrator and the administrator is prompted for the security administrator's password when each command is run.

Note:

When prompting for the security administrator's password, the following text displays: Realm management password

The password required is the Oracle ACFS security administrator's password, not the operating system password of the user.

Security administrators are allowed to browse all directories in an Oracle ACFS file system whether they have the underlying operating system permissions and whether any realm checks allow it. This functionality enables a security administrator to check the location of the files when securing them with Oracle ACFS security realms. However, a security administrator cannot view the contents of individual files without the appropriate operating system and security realm permissions.

For more information, refer to “[acfsutil sec init](#)” and “[acfsutil sec admin password](#)”.

2. Add additional security administrators as necessary.

The first security administrator can add additional security administrators to administer Oracle ACFS security with the `acfsutil sec admin add` command.

For example, add a new security administrator `medHistAdmin2`.

```
$ /sbin/acfsutil sec admin add medHistAdmin2
```

The `medHistAdmin2` user must belong to the operating system group (`medHistAdminGrp`) identified as the security administrator group with the `acfsutil sec init` command.

The `medHistAdmin2` security administrator should change the assigned temporary security password with the `acfsutil sec admin password` command. The `medHistAdmin2` administrator can add new security administrators.

For more information, refer to “[acfsutil sec admin add](#)” and “[acfsutil sec admin password](#)”.

3. Prepare an Oracle ACFS file system for security.

Run the `acfsutil sec prepare` on an Oracle ACFS file system before adding any security realms.

For example, prepare the Oracle ACFS file system mounted on `/acfsmounts/acfs1` for Oracle ACFS security.

```
$ /sbin/acfsutil sec prepare -m /acfsmounts/acfs1
```

By default, security is enabled for a file system after running this command. You can explicitly disable or enable security with the `acfsutil sec disable` or `acfsutil sec enable` commands. For more information, refer to “[acfsutil sec disable](#)” and “[acfsutil sec enable](#)”.

This command automatically creates several security realms, such as the `SYSTEM_BackupOperators` security realm. Administrators can add users to the `SYSTEM_BackupOperators` realm which gives those users permissions to make backups of realm-secured files in the Oracle ACFS file system.

For more information, refer to [“acfsutil sec prepare”](#).

4. Provide encryption for this file system.

Encrypting the file system is optional, but is enabled in this scenario.

- a.** First, run the `acfsutil encr init` command to initialize encryption and create the storage necessary for the encryption keys. This command must be run one time for each cluster on which encryption is set up.

For example, the following command initializes encryption for a cluster.

```
# /sbin/acfsutil encr init
```

This command must be run before any other encryption command and requires root or administrator privileges to run. For more information, refer to [“acfsutil encr init”](#).

- b.** Next, run the `acfsutil encr set` command to set encryption for the Oracle ACFS file system.

For example, the following command sets encryption for the file system mounted on the `/acfsmounts/acfs1` directory.

```
# /sbin/acfsutil encr set -m /acfsmounts/acfs1/
```

The `acfsutil encr set` command transparently generates a volume encryption key which is stored in the key store that was previously configured with the `acfsutil encr init` command. This command requires root or administrator privileges to run.

For more information, refer to [“acfsutil encr init”](#) and [“acfsutil encr set”](#).

5. Create a security realm on the file system.

Run the `acfsutil sec realm create` command to create a security realm for a file system.

For example, create a security realm named `medHistRealm` which contains medical records files with all files encrypted in the realm.

```
$ /sbin/acfsutil sec realm create medHistRealm -m /acfsmounts/acfs1/
-e on -a AES -k 128
```

The `-e` option specifies that all the files in the realm are encrypted with the AES algorithm and the key length set to 128 bits. The file system must first be prepared for encryption with the `acfsutil encr init` and `acfsutil encr set` commands. You do not have to enter the same value for the `-k` option with `acfsutil sec realm create` as you have entered with the `acfsutil encr set` command.

For more information, refer to [“acfsutil sec realm create”](#).

6. Create security rules.

Run the `acfsutil sec rule create` command to create rules which determine access to the files and directories of a security realm.

For example, create rules that can enable the `medMaintenance` user to access medical records for the time period 10 PM to 2 AM for file maintenance. Also, create rules that can deny operations during the time period 8 AM to 9 AM and deny operations to the `medBrowse` user.

```
$ /sbin/acfsutil sec rule create medHistRule1a -m /acfsmounts/acfs1/
-t time 22:00:00,02:00:00 -o ALLOW

$ /sbin/acfsutil sec rule create medHistRule1b -m /acfsmounts/acfs1/
-t username medMaintenance -o ALLOW

$ /sbin/acfsutil sec rule create medHistRule1c -m /acfsmounts/acfs1/
-t time 08:00:00,09:00:00 -o DENY

$ /sbin/acfsutil sec rule create medHistRule1d -m /acfsmounts/acfs1/
-t username medBrowse -o DENY
```

You can edit rules with the `acfsutil sec rule edit` command.

For more information, refer to “[acfsutil sec rule create](#)” and “[acfsutil sec rule edit](#)”.

7. Create security rule sets and add rules to rule sets.

Run the `acfsutil sec ruleset create` command to create rule sets to which rules can be added.

For example, create rule sets named `medRuleSet1` and `medRuleSet2` that include rules for operations on the files and directories of the security `medHistRealm` realm.

```
$ /sbin/acfsutil sec ruleset create medRuleSet1 -m /acfsmounts/acfs1/

$ /sbin/acfsutil sec ruleset create medRuleSet2 -m /acfsmounts/acfs1/
```

Add existing rules to the rule sets.

```
$ /sbin/acfsutil sec ruleset edit medRuleSet1 -m /acfsmounts/acfs1/
-a medHistRule1a,medHistRule1b -o ALL_TRUE

$ /sbin/acfsutil sec ruleset edit medRuleSet2 -m /acfsmounts/acfs1/
-a medHistRule1c,medHistRule1d -o ALL_TRUE
```

The `ALL_TRUE` option is the default action, but is added here to emphasize that both rules in each rule set must be true.

For more information, refer to “[acfsutil sec ruleset create](#)” and “[acfsutil sec ruleset edit](#)”.

8. Add objects to a security realm.

Run the `acfsutil sec realm add` command to add objects, such as command rules, rule sets, and files, to a security realm. For example, add the `medRuleSet1` and `medRuleSet2` rule sets and all the files in the `/acfsmounts/acfs1/medicalrecords` directory to the `medHistRealm`.

When adding a rule set to a realm, the rule set is added with a command rule, such as `DELETEFILE:medRuleSet1`. Only one rule set can be included with each command rule. To display a list of the command rules, use `acfsutil sec info` with the `-c` option. Refer to “[acfsutil sec info](#)”.

The following `acfsutil sec realm add` command enables the `medMaintenance` user to delete medical records during the time period 10 PM to 2 AM, but blocks writing to files during 8 AM to 9 AM.

```
$ /sbin/acfsutil sec realm add medHistRealm -m /acfsmounts/acfs1/
-l DELETEFILE:medRuleSet1
-f -r /acfsmounts/acfs1/medicalrecords
```

This `acfsutil sec realm add` command prevents the `medBrowse` user from writing or deleting medical records anytime.

```
$ /sbin/acfsutil sec realm add medHistRealm -m /acfsmounts/acfs1/
-l WRITE:medRuleSet2
-f -r /acfsmounts/acfs1/medicalrecords
```

This `acfsutil sec realm add` command adds backup operators to the `SYSTEM_BackupOperators` security realm that was automatically created with the `acfsutil sec prepare` command.

```
$ /sbin/acfsutil sec realm add SYSTEM_BackupOperators -m /acfsmounts/
acfs1/
-G sysBackupGrp
```

Users that belong to the `sysBackupGrp` operating system group can now make backups of realm-secured files in the Oracle ACFS file system.

For more information, refer to “[acfsutil sec realm add](#)” and “[acfsutil sec realm delete](#)”.

9. Display security information.

Run the `acfsutil sec info` command to display information for a security realm. For example, display security information for the `medHistRealm` realm.

```
$ /sbin/acfsutil sec info -m /acfsmounts/acfs1/ -n medHistRealm
```

To display the security realms to which a file or a directory belongs, run the `acfsutil sec info file` command. For example:

```
$ /sbin/acfsutil sec info file -m /acfsmounts/acfs1/
/acfsmounts/acfs1/medicalrecords
```

For more information, refer to “[acfsutil sec info](#)” and “[acfsutil sec info file](#)”.

10. Save security metadata as a backup.

Run the `acfsutil sec save` command to save the security metadata of a file system.

For example, save the security metadata of the `/acfsmounts/acfs1` file system to the `acfs1_backup.xml` file.

```
$ /sbin/acfsutil sec save -m /acfsmounts/acfs1
-p acfs1_backup.xml
```

The `acfs1_backup.xml` security metadata backup file is saved in the `/acfsmounts/acfs1/.Security/backup/` directory. The saved XML file can be loaded with the `acfsutil sec load` command.

For more information, refer to “[acfsutil sec save](#)” and “[acfsutil sec load](#)”.

You can run some `acfsutil sec` commands in a batch file with the `acfsutil sec batch` command. For example, you could create a batch file that contains a group of `acfsutil sec rule` and `acfsutil sec ruleset` commands. For more information, refer to “[acfsutil sec batch](#)”.

Auditing and diagnostic data for Oracle ACFS security is saved to log files. For more information about Oracle ACFS security, including the log files, refer to “[Oracle ACFS Security](#)”.

Encrypting Oracle ACFS File Systems

This section discusses the basic operations to manage encryption on an Oracle ACFS file system on Linux. The examples in this section show a scenario in which the medical history files are encrypted in an Oracle ACFS file system.

The steps in this section assume Oracle ACFS security is not configured for the file system; however, you can use both Oracle ACFS security and encryption on the same file system. If you decide to use both security and encryption, then both encryption and security must be initialized for the cluster containing the file system. After security is initialized on the file system, then an Oracle ACFS security administrator runs `acfsutil sec` commands to provide encryption for the file system. For information about setting up security with encryption, refer to [“Securing Oracle ACFS File Systems”](#).

Because the `acfsutil encr set` and `acfsutil encr rekey -v` commands modify the encryption key store, you should back up the Oracle Cluster Registry (OCR) after running these commands to ensure there is an OCR backup that contains all of the volume encryption keys (VEKs) for the file system.

The disk group on which the volume is created for the file system has compatibility attributes for ASM and ADVM set to 11.2.0.3 or higher. For information about disk group compatibility, refer to [“Disk Group Compatibility”](#).

For the examples in this section, various operating system users, operating system groups, and directories must exist.

The basic steps to manage encryption are:

1. Initialize encryption.

Run the `acfsutil encr init` command to initialize encryption and create the storage necessary for the encryption keys. This command must be run one time for each cluster on which encryption is set up.

For example, the following command initializes encryption for a cluster.

```
# /sbin/acfsutil encr init
```

This command must be run before any other encryption command and requires root or administrator privileges to run.

For more information, refer to [“acfsutil encr init”](#).

2. Set encryption parameters.

Run the `acfsutil encr set` command to set the encryption parameters for the entire Oracle ACFS file system.

For example, the following command sets the AES encryption algorithm and a file key length of 128 for a file system mounted on the `/acfsmounts/acfs1` directory.

```
# /sbin/acfsutil encr set -a AES -k 128 -m /acfsmounts/acfs1/
```

The `acfsutil encr set` command also transparently generates a volume encryption key which is stored in the key store that was previously configured with the `acfsutil encr init` command.

This command requires root or administrator privileges to run.

For more information, refer to [“acfsutil encr set”](#).

3. Enable encryption.

Run the `acfsutil encr on` command to enable encryption for directories and files.

For example, the following command enables encryption recursively on all files in the `/acfsmounts/acfs1/medicalrecords` directory.

```
# /sbin/acfsutil encr on -r /acfsmounts/acfs1/medicalrecords
                        -m /acfsmounts/acfs1/
```

For users that have appropriate permissions to access files in the `/acfsmounts/acfs1/medicalrecords` directory, they can still read the decrypted files.

This command can be run by an administrator or the file owner.

For more information, refer to “[acfsutil encr on](#)”.

4. Display encryption information.

Run the `acfsutil encr info` command to display encryption information for directories and files.

```
# /sbin/acfsutil encr info -m /acfsmounts/acfs1/
                        -r /acfsmounts/acfs1/medicalrecords
```

This command can be run by an administrator or the file owner.

For more information, refer to “[acfsutil encr info](#)”.

Auditing and diagnostic data for Oracle ACFS encryption is saved to log files. For more information about Oracle ACFS encryption, including the log files, refer to “[Oracle ACFS Encryption](#)”.

Tagging Oracle ACFS File Systems

This section discusses the operations to manage tagging on directories and files in an Oracle ACFS file system on Linux.

The disk group on which the volume is created for the file system has compatibility attributes for ASM and ADVM set to 11.2.0.3 or higher. For information about disk group compatibility, refer to “[Disk Group Compatibility](#)”.

Oracle ACFS implements tagging with Extended Attributes. There are some requirements for using Extended Attributes; refer to “[Oracle ACFS Tagging](#)”.

The steps to manage tagging are:

1. Specify tag names for directories and files.

Run the `acfsutil tag set` command to set tags on directories or files. You can use these tags to specify which objects are replicated.

For example, add the `comedy` and `drama` tags to the files in the subdirectories of the `/acfsmounts/repl_data/films` directory.

```
$ /sbin/acfsutil tag set -r comedy /acfsmounts/repl_data/films/comedies
$ /sbin/acfsutil tag set -r drama /acfsmounts/repl_data/films/dramas
$ /sbin/acfsutil tag set -r drama /acfsmounts/repl_data/films/mysteries
```

In this example, the `drama` tag is purposely used twice and that tag is changed in a later step.

You must have system administrator privileges or be the file owner to run this command.

For more information, refer to [“acfsutil tag set”](#).

2. Display tagging information.

Run the `acfsutil tag info` command to display the tag names for directories or files in Oracle ACFS file systems. Files without tags are not displayed.

For example, display tagging information for files in the `/acfsmounts/repl_data/films` directory.

```
$ /sbin/acfsutil tag info -r /acfsmounts/repl_data/films
```

Display tagging information for files with the `drama` tag in the `/acfsmounts/repl_data/films` directory.

```
$ /sbin/acfsutil tag info -t drama -r /acfsmounts/repl_data/films
```

You must have system administrator privileges or be the file owner to run this command.

For more information, refer to [“acfsutil tag info”](#).

3. Remove and change tag names if necessary.

Run the `acfsutil tag unset` command to remove tags on directories or files. For example, unset the `drama` tag on the files in the `mysteries` subdirectory of the `/acfsmounts/repl_data/films` directory to apply a different tag to the subdirectory.

```
$ /sbin/acfsutil tag unset -r drama /acfsmounts/repl_data/films/mysteries
```

Add the `mystery` tag to the files in the `mysteries` subdirectory of the `/acfsmounts/repl_data/films` directory.

```
$ /sbin/acfsutil tag set -r mystery /acfsmounts/repl_data/films/mysteries
```

You must have system administrator privileges or be the file owner to run these commands.

For more information, refer to [“acfsutil tag unset”](#).

For more information about tagging an Oracle ACFS file system, refer to [“Oracle ACFS Tagging”](#).

Replicating Oracle ACFS File Systems

This section discusses the operations to manage replication on an Oracle ACFS file system on Linux.

The disk groups on which volumes are created for the primary and standby file systems must have compatibility attributes for ASM and ADVM set to `11.2.0.3` or higher. For information about disk group compatibility, refer to [“Disk Group Compatibility”](#).

The steps to manage replication are:

1. Determine the storage capacity necessary for replication on the sites hosting the primary and standby file systems. The primary file system must have a minimum size of 4 GB for each node that is mounting the file system. The standby file system must have a minimum size of 4 GB and should be sized appropriately for

the amount of data being replicated and the space necessary for the replication logs sent from the primary file system.

Calculate the replication-related storage requirement for the primary file system, then use the same size requirement for the standby file system. If Oracle ACFS tagging is used to replicate only a subset of the files in the primary file system, then the size requirement for the standby file system is proportional to that subset of the primary file system.

Run the `acfsutil info fs` command with the `-s interval` option on the node where the primary file system is mounted to display the amount and rate of change to the primary file system for the node. The amount of change includes all user and metadata modifications to the primary file system. This amount approximates the size of replication logs that are generated when recording changes to the file system. Changes are stored in temporary files called replication logs which are kept in a special directory in the primary file system until they can be sent to the standby to be applied. After confirmation is received that the changes contained in a replication log have been successfully applied to the standby file system, the replication logs on the primary file system are deleted.

To approximate the extra storage capacity necessary for the replication logs, determine the following:

- The time interval during which the site hosting the primary file system may experience network connectivity problems or slowdowns when accessing the site hosting the standby file system.
- The time interval during which the site hosting the standby file system may be taken offline for maintenance.

These time intervals are used in calculating the amount and rate of change in storage space. You must account for the time interval when the primary file system cannot send the replication logs over to the standby file system at its usual rate or when standby file systems are inaccessible while undergoing maintenance. The replication logs continue to accumulate on the site hosting the primary file system and may eventually cause that site to run out of space.

For the following scenario, assume $t = 60$ minutes is the time interval in your environment that would adequately account for network problems or maintenance on site hosting the standby file system.

Run `acfsutil info fs -s 900` on the primary file system to collect the average rate of change over a 24 hour period with a 15 minute (900 seconds) interval. The $t/4$ ($60/4=15$) result is the value for the sampling interval. Do not exceed a value of $t/2$ for the time interval as you may miss some important peaks.

```
$ /sbin/acfsutil info fs -s 900 /acfsmounts/repl_data
```

With the output, you can determine the average rate of change, the peak rate of change, and how long the peaks last. However, the command displays information only for the node on which the command is run. To collect the total amount of change in the file system the command must be run on every node that is modifying the file system. The maximum number of supported nodes is eight.

The following formula approximates the extra storage capacity needed:

$$\text{Extra storage capacity to hold replication logs} = (\text{Number-nodes-on-primary} * 1\text{GB}) + P$$

where P is the peak amount of change generated across all nodes for time t as reported by the `acfsutil info fs -s` output.

In the example, you must total the changes from four 15-minute intervals to find the total amount of change that could occur in 60 minutes. You may choose to use the single hour that generated the largest amount of change, or you could select the top four 15-minute intervals even if they did not occur together to prepare for the worst-case scenario.

Assume that you have four nodes modifying the primary file system, and that during the measured interval, the peak amount of change reported for the 60 minutes is approximately 20 GB for all nodes. Using the storage capacity formula, 24 GB of excess storage capacity on each site hosting the primary file system is required for storage of the replication logs.

```
Extra storage capacity to hold replication logs = (4 * 1GB per node) +
20GB maximum change per hour = 24GB of extra storage capacity
```

Next, check that the network transfer rate is greater than or equal to the rate of change observed during the monitoring period. In the previous example, the peak of 20 GB of changed data per hour is equivalent to a peak rate of change of about 5.5 MB/sec. To keep up with this rate of change, you must ensure that the network can reliably transfer at least this amount of data per second without negatively impacting your existing network workloads.

To estimate your current actual network transfer rate, calculate the elapsed time required to FTP a 1 GB file from the primary file system to the intended standby file system during an interval when network usage is low. For example, if the 1 GB file transfers in 30 seconds, then your current FTP transfer rate is 33 MB per seconds (1000 MB/30 seconds = 33 MB per second). Because of various delays inherent in the transfers, for planning purposes you should reduce this measured FTP transfer rate by 20%, and then by an additional 5% per node.

In the previous example with 4 nodes, the FTP transfer rate used for planning is:

```
33 MB/sec * (1 - (0.2) - (4 * 0.05)) = 33 * (0.6) = ~20MB/sec
```

Because the peak rate of change was only 5.5 MB/second, you can expect the network to be able to handle this additional workload in this example. However, if the network capacity is close to fully utilized, you might want to consider increasing network capacity before implementing replication for this file system and workload.

In addition, insure you have sufficient network capacity to allow replication to catch up after times when network problems prevent a primary file system from sending replication logs to the standby file system.

For more information, refer to "[acfsutil info fs](#)".

2. Set up tags, user names, and service names.

When starting replication on an Oracle ACFS file system, first perform the following steps:

- Determine the user name and password that the sites hosting the primary and standby file systems use to connect to the remote Oracle ASM instance as the Oracle ASM and DBA administrator. All nodes that have the file system mounted must support this user name and password. The user must have SYSASM and SYSDBA privileges. For example:

```
SQL> CREATE USER primary_admin IDENTIFIED BY primary_passwd;
SQL> GRANT sysasm,sysdba TO primary_admin;
```

Oracle wallets should be used to manage security credentials.

See Also:

- *Oracle Database Enterprise User Security Administrator's Guide* for information about Oracle wallets
 - *Oracle Database SecureFiles and Large Objects Developer's Guide* for information about wallet management
 - *Oracle Database Net Services Reference* for information about wallet parameters in the `SQLNET.ORA` file
-

- Determine a unique service name for the replicated file system.

When both the primary and standby file systems are located in different clusters for disaster tolerance, then the service names for the primary and standby file systems can be the same. However, if the both file systems are mounted on the same node, such as a test configuration, then unique service names must be used for the primary and standby file systems. Using unique service names for the primary and standby file systems requires the use of the `-c` option during replication initialization. Service names are limited to a maximum of 128 bytes.

Note:

- You must specify a service name other than `+ASM` because that service name is currently in use by the Oracle ASM instance.
 - You must specify a unique service name for each file system that you want to replicate when there are multiple replicated file systems on a node or cluster.
-

Using this service name, create a net service alias on the sites hosting the primary and standby file system that connects to the remote site. This alias along with the user name and password are used as the connection string in the replication initialization commands.

For example, the following are examples of connect descriptors with net service aliases for the sites hosting the primary and standby file systems.

```
primary_repl_site=(DESCRIPTION=
  (ADDRESS=(PROTOCOL=tcp)(HOST=primary1.example.com)(PORT=1521))
  (ADDRESS=(PROTOCOL=tcp)(HOST=primary2.example.com)(PORT=1521))
  (CONNECT_DATA=(SERVICE_NAME=primary_service)))

standby_repl_site=(DESCRIPTION=
  (ADDRESS=(PROTOCOL=tcp)(HOST=standby1.example.com)(PORT=1521))
  (CONNECT_DATA=(SERVICE_NAME=standby_service)))
```

If you want to perform replication using a single client access name (SCAN) VIP, you must update the `REMOTE_LISTENER` initialization parameter in the Oracle ASM instance before initializing replication. You can update the parameter in the initialization file or with the `ALTER SYSTEM SQL` statement.

For example:

```
SQL> ALTER SYSTEM SET remote_listener='SCAN_NAME:1521' sid='*'
scope=both;
```


See Also:

Oracle Database Net Services Administrator's Guide for information about connect descriptors

- Optionally set tags on directories and files to replicate only selected files in an Oracle ACFS file system. You can also add tags to files after replication has started. For information about the steps to tag files, refer to “[Tagging Oracle ACFS File Systems](#)”.
3. Configure the site hosting the standby file system.

Before replicating an Oracle ACFS file system, configure the site hosting the standby file system by performing the following procedures.

- Create a new file system of adequate size to hold the replicated files and associated replication logs from the primary file system. For example: `/standby/repl_data`
- Mount the file system on one node only.
- Run the `acfsutil repl init standby` command. If this command is interrupted for any reason, the user must re-create the file system, mount it on one node only, and rerun the command. This command requires the following configuration information:

- The connect string to be used to connect to the site hosting the primary file system. For example:

```
/@primary_repl_site
```

The connect string searches in the user's wallet for the user name and password associated with the alias `primary_repl_site`. The user must have `SYSASM` and `SYSDBA` privileges.

- If the standby file system is using a different service name than the primary file system, then the use `-c` option. This option specifies the service name for the standby file system. For example:

```
standby_repl_service
```

- The mount point of the standby file system. For example:

```
/standby/repl_data
```

For example, run the following `acfsutil repl init standby` command on the site hosting the standby file system.

```
$ /sbin/acfsutil repl init standby
  -p /@primary_repl_site
  -c standby_repl_service /standby/repl_data
```

The `acfsutil repl init standby` command requires root or system administrator privileges to run.

For more information, refer to “[acfsutil repl init](#)”.

4. Configure the site hosting the primary file system.

After the standby file system has been set up, configure the site hosting the primary file system and start replication by performing the following procedures.

Run the `acfsutil repl init primary` command. This command requires the following configuration information:

- The connect string to be used to connect to the site hosting the standby file system. For example:
`/@standby_repl_site`
The connect string searches in the user's wallet for the user name and password associated with the alias `standby_repl_site`. The user must have `SYSASM` and `SYSDBA` privileges.
- The mount point of the primary file system. For example: `/acfsmounts/repl_data`
- If the primary file system is using a different service name than the standby file system, then use the `-c` option. This option specifies the service name on the site hosting the primary file system. For example:
`primary_repl_service`
- If the mount point is different on the site hosting the standby file system than it is on the site hosting the primary file system, specify the mount point on the standby file system with the `-m standby_mount_point` option. For example:
`-m /standby/repl_data`

For example, run the following `acfsutil repl init primary` command on the site hosting the primary file system.

```
$ /sbin/acfsutil repl init primary
  -s /@standby_repl_site
  -m /standby/repl_data -c primary_repl_service
  /acfsmounts/repl_data
```

The `acfsutil repl init primary` command requires root or system administrator privileges to run.

For more information, refer to “[acfsutil repl init](#)”.

5. Monitor information about replication on the file system.

The `acfsutil repl info` command displays information about the state of the replication processing on the primary or standby file system.

For example, run the following `acfsutil repl info` command on the site hosting the primary file system to display configuration information.

```
$ /sbin/acfsutil repl info -c -v /acfsmounts/repl_data
```

You must have system administrator or Oracle ASM administrator privileges to run this command.

For information, refer to “[acfsutil repl info](#)”.

6. Manage replication background processes.

Run the `acfsutil repl bg` command to start, stop, or retrieve information about replication background processes.

For example, the following example displays information about the replication processes for the `/acfsmounts/repl_data` file system.

```
$ /sbin/acfsutil repl bg info /acfsmounts/repl_data
```

You must have system administrator or Oracle ASM administrator privileges to run the `acfsutil repl bg info` command.

For more information, refer to “[acfsutil repl bg](#)”.

7. Pause replication momentarily only if necessary.

Run the `acfsutil repl pause` to momentarily stop replication. You should run the `acfsutil repl resume` command soon as possible to resume replication.

For example, the following command pauses replication on the `/acfsmounts/repl_data` file system.

```
$ /sbin/acfsutil repl pause /acfsmounts/repl_data
```

The following command resumes replication on the `/acfsmounts/repl_data` file system.

```
$ /sbin/acfsutil repl resume /acfsmounts/repl_data
```

You must have system administrator or Oracle ASM administrator privileges to run these commands.

For more information, refer to “[acfsutil repl pause](#)” and “[acfsutil repl resume](#)”.

8. Failing over to a standby or turning a standby file system into an active file system.

If the primary file system is gone, you can run the `acfsutil terminate standby mount_point` command to turn the standby file system into an active file system. If the primary file system still exists, you should terminate the primary first with `acfsutil terminate primary mount_point`.

Before terminating replication with `acfsutil repl terminate` on the standby file system, you can determine the point in time of the primary file system that the standby file system represents. This timestamp is displayed with the `acfsutil repl info -c` command as `Last sync time with primary`. If the failover action must be coordinated with Oracle Data Guard, you can use the timestamp to set back the database if needed or perform other necessary actions that are based on the time stamp. For information, refer to “[acfsutil repl info](#)”.

Note:

On an Oracle ACFS file system `df` reports space usage by internal metadata plus user files and directories. `du` only reports the space usage of user files and directories. Depending on the size of the volume and number of the nodes, internal metadata is allocated in varying sizes. Additionally, with replication enabled an internal replication log is allocated for each node that is used to record changes to the file system before exposing the replication log to user space daemons to transport to the standby.

For more information about replicating an Oracle ACFS file system, refer to “[Oracle ACFS Replication](#)”.

Deregistering, Dismounting, and Disabling Volumes and Oracle ACFS File Systems

This section discusses the operations to deregister or dismount a file system and disable a volume. This section contains these topics:

- [Deregistering an Oracle ACFS File System](#)
- [Dismounting an Oracle ACFS File System](#)
- [Disabling a Volume](#)

Deregistering an Oracle ACFS File System

You can deregister an Oracle ACFS file system if you do not want the file system to be automatically mounted.

For example:

```
$ /sbin/acfsutil registry -d /acfsmounts/acfs1
```

If you deregister a file system, then you must explicitly mount the file system after Oracle Clusterware or the system is restarted.

For more information about the registry, see [“About the Oracle ACFS Mount Registry”](#). For information about `acfsutil registry`, see [“acfsutil registry”](#).

Dismounting an Oracle ACFS File System

You can dismount a file system without deregistering the file system or disabling the volume on which the file system is mounted.

For example, you can dismount a file system and run `fsck` to check the file system.

```
# /bin/umount /acfsmounts/acfs1  
  
# /sbin/fsck -a -v -y -t acfs /dev/asm/volume1-123
```

After you dismount a file system, you must explicitly mount the file system.

Use `umount` on Linux systems or `acfsdismount` on Windows systems. For information about the commands to dismount a file system, see [“umount”](#) or [“acfsdismount”](#).

Use `fsck` on Linux systems or `acfschkdsk` on Windows systems to check a file system. For information about the commands to check a file system, see [“fsck”](#) or [“acfschkdsk”](#).

Disabling a Volume

To disable a volume, you must first dismount the file system on which the volume is mounted.

For example:

```
# /bin/umount /acfsmounts/acfs1
```

After a file system is dismounted, you can disable the volume and remove the volume device file.

For example:

```
ASMCMDB> voldisable -G data volume1
```

Dismounting the file system and disabling a volume does not destroy data in the file system. You can enable the volume and mount the file system to access the existing data. For information about `voldisable` and `volenable`, see [Managing Oracle ADVM with ASMCMDB](#).

Removing an Oracle ACFS File System and a Volume

To permanently remove a volume and Oracle ACFS file system, perform the following steps. These steps destroy the data in the file system.

1. Deregister the file system with `acfsutil registry -d`.

For example:

```
$ /sbin/acfsutil registry -d /acfsmounts/acfs1
acfsutil registry: successfully removed ACFS mount point
/acfsmounts/acfs1 from Oracle Registry
```

For information about running `acfsutil registry`, see [“acfsutil registry”](#).

2. Dismount the file system.

For example:

```
# /bin/umount /acfsmounts/acfs1
```

You must dismount the file system on all nodes of a cluster.

Use `umount` on Linux systems or `acfsdismount` on Windows systems. For information about running `umount` or `acfsdismount`, see [“umount”](#) or [“acfsdismount”](#).

3. Remove the file system with `acfsutil rmfs`.

If you were not planning to remove the volume in a later step, this step is necessary to remove the file system. Otherwise, the file system is removed when the volume is deleted.

For example:

```
$ /sbin/acfsutil rmfs /dev/asm/volume1-123
```

For information about running `acfsutil rmfs`, see [“acfsutil rmfs”](#).

4. Optionally you can disable the volume with the ASMCMD `voldisable` command.

For example:

```
ASMCMD> voldisable -G data volume1
```

For information about running `voldisable`, see [Managing Oracle ADVM with ASMCMD](#).

5. Delete the volume with the ASMCMD `volddelete` command.

For example:

```
ASMCMD> volddelete -G data volume1
```

For information about running `volddelete`, see [Managing Oracle ADVM with ASMCMD](#).

Oracle ACFS Command-line Tools for Linux Environments

[page 16-22](#) contains a summary of the Oracle ACFS commands for Linux environments. The commands in [page 16-22](#) have been extended with additional

options to support Oracle ACFS. All other Linux file system commands operate without change for Oracle ACFS.

For example, Oracle ACFS adds a set of Oracle ACFS-specific mount options to those provided with the base operating system platform. You should review both the mount options for the Linux platforms in addition to the Oracle ACFS-specific options for the complete set of file system mount options.

File systems on Oracle ADVM volumes that are not Oracle ACFS file systems, such as `ext3`, are managed with the same Linux commands that are listed in [page 16-22](#) using the file-specific options for the type of file system. You can refer to the `man` pages for options available for the Linux commands in [page 16-22](#).

Note:

When using Security-Enhanced Linux (SELinux) in enforcing mode with Oracle ACFS, ensure that the Oracle ACFS file systems are mounted with an SELinux default context. Refer to your Linux vendor documentation for information about the context mount option.

Command	Description
fsck	Checks and repairs an Oracle ACFS file system.
mkfs	Creates an Oracle ACFS file system.
mount	Mounts an Oracle ACFS file system.
umount	Dismounts an Oracle ACFS file system.

fsck

Purpose

Checks and repairs an Oracle ACFS file system.

Syntax and Description

```
fsck -t acfs -h /dev/null
fsck [-a|-f] [-v] -t acfs [-n|-y] volume_device
```

`fsck -t acfs -h /dev/null` displays usage text and exits.

[Table 2](#) contains the options available with the `fsck` command.

Table 2 Options for the Linux `fsck` command

Option	Description
<code>-a</code>	Specifies to automatically repair the file system.
<code>-f</code>	Forces the file system into mountable state without completing a file system check or repair.
<code>-v</code>	Specifies verbose mode. The progress is displayed as the operation occurs. Running in verbose mode can impact performance.
<code>-h</code>	Displays the usage help text and exits.

Option	Description
-n	Answers no to any prompts.
-y	Answers yes to any prompts.
<i>volume_device</i>	Specifies the primary Oracle ADVM volume device.

`fsck` checks and repairs an existing Oracle ACFS. This command can only be run on a dismounted file system. `root` privileges are required to run `fsck`. The Oracle ACFS driver must be loaded for `fsck` to work.

By default, `fsck` only checks for and reports any errors. The `-a` flag must be specified to instruct `fsck` to repair errors in the file system. Do not interrupt `fsck` during the repair operation.

In a few cases, `fsck` prompts for questions before proceeding to check a file system. These cases include:

- If `fsck` detects that another `fsck` is in progress on the file system
- If `fsck` detects that the Oracle ACFS driver is not loaded
- If the file system does not appear to be Oracle ACFS

In checking mode, `fsck` also prompts if there are transaction logs that have not been processed completely due to an incomplete shutdown. To run in a non-interactive mode, include either the `-y` or `-n` options to answer yes or no to any questions.

`fsck` creates working files before it checks a file system. These working files are created in `/usr/tmp` if space is available. `/tmp` is used if `/usr/tmp` does not exist. If insufficient space is available in the `tmp` directory, `fsck` attempts to write to the current working directory. The files that `fsck` creates are roughly the size of the file system being checked divided by 32K. At most three such files are allocated. For example, a 2 GB file system being checked causes `fsck` to generate one to three 64K working files in the `/usr/tmp` directory. These files are deleted after `fsck` has finished.

In the event that `fsck` finds a file or directory in the file system for which it cannot determine its name or intended location (possibly due to a corruption in its parent directory), it places this object in the `/lost+found` directory when `fsck` is run in `fix` mode. For security reasons only the `root` user on Linux can read files in `/lost+found`. If the administrator can later determine the original name and location of the file based on its contents, the file can be moved or copied into its intended location.

The file names in the `/lost+found` directory are in the following formats:

```
parent.id.file.id.time-in-sec-since-1970
parent.id.dir.id.time-in-sec-since-1970
```

The `id` fields are the internal Oracle ACFS numeric identifiers for each file and directory in the file system.

You can use `acfsutil info id id mount_point` to attempt to determine the directory associated with `parent.id`. This directory is assumed to be where the deleted object originated. For information about `acfsutil info`, see “[acfsutil info file](#)”.

If the parent directory is not known, the `parent id` field is set to UNKNOWN.

Note:

It is not possible to see the contents of the `/lost+found` directory from a snapshot.

Examples

The following example shows how to check and repair an Oracle ACFS file system.

Example 1 Using the fsck command

```
# /sbin/fsck -a -y -t acfs /dev/asm/volume1-123
```

mkfs**Purpose**

Creates an Oracle ACFS file system.

Syntax and Description

```
mkfs -t acfs -h
mkfs [-v] [-f]-t acfs [-n name ] volume_device [-a accelerator_volume] [size]
```

`mkfs -t acfs -h` displays usage text and exits.

[Table 3](#) contains the options available with the `mkfs` command.

Table 3 Options for the Linux mkfs command

Option	Description
<code>-t acfs</code>	Specifies the type of file system on Linux. <code>acfs</code> designates the Oracle ACFS type.
<code>-v</code>	Specifies verbose mode. The progress is displayed as the operation occurs.
<code>-n name</code>	Specifies the name for the file system. A name can be a maximum of 64 characters. <code>acfsutil info fs</code> returns the name if one was specified.
<code>-f</code>	Specifies the force option. This action creates the file system even if there is an existing Oracle ACFS on the volume device, although only if the file system is dismounted. This option overwrites structures on the original file system. Use this option with caution.
<code>-h</code>	Displays the usage help text and exits.
<code>size</code>	Specifies the size that the file system should consume on the named device. The quantity specified can be in units of <code>K</code> (kilobytes), <code>M</code> (megabytes), <code>G</code> (gigabytes), <code>T</code> (terabytes), or <code>P</code> (petabytes). If a unit is not specified, the default is bytes. If this option is not specified, the entire device is consumed.
<code>volume_device</code>	Specifies an existing Oracle ADVM device file that is to be formatted. This device is the primary volume.
<code>-a accelerator_volume</code>	Specifies a secondary Oracle ACFS accelerator volume that is used by Oracle ACFS to store critical metadata.

You can use `mkfs` to create the on disk structure needed for Oracle ACFS file system to be mounted. The `mkfs` command is the traditional Linux command used to build a file system. After `mkfs` runs successfully, the `USAGE` column in the `V$ASM_VOLUME` view displays `ACFS`. `root` privilege is not required. The ownership of the volume device file dictates who can run this command. Oracle ADVM volumes are created with the `ASMCMD volcreate` command. For information about the `volcreate` command, refer to “[volcreate](#)”.

The minimum file system size is 200 MB. The Oracle ACFS driver must be loaded for `mkfs` to operate successfully.

Oracle ACFS Accelerator Volume

Note:

This feature is included starting with Oracle Database 12c Release 1 (12.1.0.2). The feature is reserved for future use. Oracle ACFS accelerator volume currently provides no performance gain in 12.1.0.2.

Use an accelerator volume to reduce the time to access the Oracle ACFS metadata log, which is located on the accelerator volume. The accelerator volume is created with the `-a` option with the `mkfs` command. The value of `COMPATIBLE.ADVM` must be at least 12.1.0.2 to use the `-a` option.

Create the accelerator volume on a disk group with storage that is significantly faster than the primary volume's storage. For example, Solid State Disk (SSD) storage could be used. The size of the accelerator volume should be at least 32 MB for each node in the cluster. For example, in an eight-node cluster the recommended minimum size of the accelerator volume is 256 MB. If an accelerator volume is smaller than the recommended size, the file system can operate normally, but the full benefit of the storage accelerator may not be achieved. The minimum size of the accelerator volume is 128 MB. Oracle ADVM volumes are created with the `ASMCMD volcreate` command. For information about the `volcreate` command, refer to “[volcreate](#)”.

The accelerator volume is linked to the primary volume specified with the `mkfs` command. When mounting a file system, only the primary volume is specified. If the accelerator volume becomes inaccessible for any reason after a file system with the volume is mounted, the file system is taken offline. Only one storage accelerator volume can be associated with an Oracle ACFS file system. After an accelerator volume is associated with a file system, the volume cannot be disassociated from the file system. The accelerator volume cannot be resized.

Examples

Before creating an Oracle ACFS file system, first determine which Oracle ADVM volume devices are available. You can use the `ASMCMD volinfo` command to display information about the volumes and volume devices.

```
ASMCMD [+] > volinfo -a
...
      Volume Name: VOLUME1
      Volume Device: /dev/asm/volume1-123
      State: ENABLED
...
```

For information about the `volcreate` and `volinfo` commands, refer to [Managing Oracle ADVM with ASMCMD](#).

Next create an Oracle ACFS file system on a volume device file.

Example 2 Using the mkfs command

```
$ /sbin/mkfs -t acfs /dev/asm/volume1-123
```

```
$ /sbin/mkfs -t acfs /dev/asm/volume1-127 -a /dev/asm/volume2-130
```

mount

Purpose

Mounts an Oracle ACFS file system.

Syntax and Description

```
mount -h
mount [-v] -n -t acfs [-o options] volume_device mount_point
mount
```

`mount -h` displays usage text and exits.

[Table 4](#) contains the options available with the `mount` command.

Table 4 Options for the Linux mount command

Option	Description
-h	Displays the usage help text and exits.
-t acfs	Specifies the type of file system on Linux. <code>acfs</code> designates the Oracle ACFS type.
-v	Specifies verbose mode. The progress is displayed as the operation occurs.
-n	Specifies not to update the <code>/etc/mtab</code> file.
-o	Options are specified with the <code>-o</code> flag followed by a comma-delimited string of options. The following options are available: <ul style="list-style-type: none"> • <code>all</code> Reads the Oracle ACFS managed file systems in the Oracle Clusterware namespace, mounting all file systems with the <code>AUTO_START=always</code>. When the <code>-o all</code> option is specified, other <code>-o</code> options are ignored. To specify mount options for a registry entry, include those options with the <code>acfsutil registry</code> command when you add the entry to the registry. • <code>ro</code> Mounts the file system in read-only mode. • <code>norootsuid</code> Fails the execution of binaries by non-root users whose permissions allow set user Id execution, and are owned by root. An attempt to run these executables as a non-root user fails with a permission denied error. • <code>rootsuid</code> Allows the execution of binaries by non-root users of set user Id files owned by root. This is the default action.

Option	Description
<i>volume_device</i>	Specifies a primary Oracle ADVM volume device file that has been formatted by <i>mkfs</i> . <i>device</i> is required but can be a dummy value.
<i>mount_point</i>	Specifies the directory where the file system is mounted. This directory must exist before you run the <code>mount</code> command.

`mount` attaches a file system to the Oracle ACFS hierarchy at the mount point that is the name of a directory. The mount happens on the node where the mount command was issued. The mount command returns an error if the file system is not in a dismounted state on this node.

It is not always possible to return the cause of a mount failure to the `mount` command. When this happens Oracle ACFS writes the cause of the failure to the system console and associated system log file.

After `mount` runs successfully, the `MOUNTPATH` field in the `V$ASM_VOLUME` view displays the directory name on which the file system is now mounted.

An Oracle ACFS file system should only be mounted on one mount point. The same mount point name should be used on all cluster members.

The `mount` command lists all mounted file systems if it is run with no parameters. `root` privilege is required to run `mount`.

Examples

The first example shows how to mount `volume1-123` on the mount point `/acfsmounts/acfs1`. The second example shows how to mount all the registered Oracle ACFS file systems. The dummy names (`none`) have been entered for the device and directory as they are required, but not used, when the `all` option is specified.

Example 3 Using the mount command

```
# /bin/mount -t acfs /dev/asm/volume1-123 /acfsmounts/acfs1
# /bin/mount -t acfs -o all none none
```

umount

Purpose

Dismounts an Oracle ACFS file system.

Syntax and Description

```
umount -h
umount [-v] -l -n volume_device |mount_point
umount -a -l -n [-t acfs]
```

`umount -h` displays usage text and exits.

[Table 5](#) contains the options available with the `umount` command.

Table 5 Options for the Linux `umount` command

Option	Description
<code>-h</code>	Displays the usage help text and exits.

Option	Description
<code>-t acfs</code>	Specifies the type of file system on Linux. <code>acfs</code> designates the Oracle ACFS type.
<code>-v</code>	Specifies verbose mode. The progress is displayed as the operation occurs.
<code>-a</code>	Specifies to dismount all Oracle ACFS file systems on this node.
<code>-l</code>	Specifies a lazy unmount. The Oracle ACFS file system is dismounted, but the cleanup of all references to the file system occurs when the system is no longer busy.
<code>-n</code>	Specifies not to update the <code>/etc/mtab</code> file.
<code>volume_device</code>	Specifies an Oracle ADVM volume device file that has been formatted by <code>mkfs</code> .
<code>mount_point</code>	Specifies the directory where the file system is mounted. This directory must exist before you run the <code>mount</code> command.

`umount` detaches an Oracle ACFS from the file system hierarchy on the current node. If the file system is busy, `umount` fails.

root privileges are required to run the `umount` command.

Examples

The following examples show how to dismount an Oracle ACFS file system. The first example uses the volume device file and the second example uses the file system.

Example 4 Using the `umount` command

```
# /bin/umount /dev/asm/volume1-123
# /bin/umount /acfsmounts/acfs1
```

Oracle ACFS Command-line Tools for the Solaris Environment

Note:

If a disk group is dismounted with the force option on Solaris, any Oracle ADVM volumes device files that were on that disk group remain on the system. These files are removed when the disk group is remounted.

[page 16-28](#) contains a summary of the Oracle ACFS commands for Solaris. The commands in [page 16-28](#) have been extended with additional options to support Oracle ACFS on Solaris.

Command	Description
fsck	Checks and repairs an Oracle ACFS file system on Solaris.
mkfs	Creates an Oracle ACFS file system on Solaris.
mount	Mounts an Oracle ACFS file system on Solaris.
umount/umountall	Dismounts an Oracle ACFS file system on Solaris.

fsck

Purpose

Checks and repairs an Oracle ACFS file system on the Solaris operating system.

Syntax and Description

```
fsck -F acfs -o h /dev/null
fsck -F acfs [{-n|N}|{-y|Y}] [-o options] volume_device
```

`fsck -F acfs -o h /dev/null` displays usage text and exits.

[Table 7](#) contains the options available with the `fsck` command.

Table 7 Options for the Solaris `fsck` command

Option	Description
<code>-F acfs</code>	Specifies the type of file system on Solaris. <code>acfs</code> designates the Oracle ACFS type.
<code>-n N</code>	Answers no to any prompts.
<code>-y Y</code>	Answers yes to any prompts.
<code>-o</code>	Specifies that options follow (<code>a</code> , <code>f</code> , <code>h</code> , <code>v</code>). Options are preceded with the <code>-o</code> flag and entered as a comma-delimited string. For example: <code>-o a,v</code> <ul style="list-style-type: none"> • <code>a</code> Specifies to automatically fix the file system. • <code>f</code> Forces the file system into mountable state without completing a file system check or fix. • <code>h</code> Displays the usage text and exits. • <code>v</code> Specifies verbose mode. The progress is displayed as the operation occurs. Running in verbose mode can impact performance.
<code>volume_device</code>	Specifies an Oracle ADVM device file.

`fsck` checks and repairs an existing Oracle ACFS file system. This command can only be run on a dismounted file system. `root` privileges are required to run `fsck`. The Oracle ACFS driver must be loaded for `fsck` to work.

By default, `fsck` only checks for and reports any errors. The `-o a` option must be specified to instruct `fsck` to fix errors in the file system. Do not interrupt `fsck` during the repair operation.

In a few cases, `fsck` prompts for questions before proceeding to check a file system. These cases include:

- If `fsck` detects that another `fsck` is in progress on the file system
- If `fsck` detects that the Oracle ACFS driver is not loaded
- If the file system does not appear to be Oracle ACFS

In checking mode, `fsck` also prompts if there are transaction logs that have not been processed completely due to an incomplete shutdown. To run in a non-interactive mode, include either the `-y` or `-n` options to answer yes or no to any questions.

`fsck` creates working files before it checks a file system. These working files are created in `/usr/tmp` if space is available. `/tmp` is used if `/usr/tmp` does not exist. If insufficient space is available in the `tmp` directory, `fsck` attempts to write to the current working directory. The files that `fsck` creates are roughly the size of the file system being checked divided by 32K. At most three such files are allocated. For example, a 2 GB file system being checked causes `fsck` to generate one to three 64K working files in the `/usr/tmp` directory. These files are deleted after `fsck` has finished.

In the event that `fsck` finds a file or directory in the file system for which it cannot determine its name or intended location (possibly due to a corruption in its parent directory), it places this object in the `/lost+found` directory when `fsck` is run in fix mode. For security reasons only the `root` user on Linux can read files in `/lost+found`. If the administrator can later determine the original name and location of the file based on its contents, the file can be moved or copied into its intended location.

The file names in the `/lost+found` directory are in the following formats:

```
parent.id.file.id.time-in-sec-since-1970
parent.id.dir.id.time-in-sec-since-1970
```

The `id` fields are the internal Oracle ACFS numeric identifiers for each file and directory in the file system.

You can use `acfsutil info id id mount_point` to attempt to determine the directory associated with `parent.id`. This directory is assumed to be where the deleted object originated. For information about `acfsutil info`, see "[acfsutil info file](#)".

If the parent directory is not known, the parent `id` field is set to UNKNOWN.

Note:

It is not possible to see the contents of the `/lost+found` directory from a snapshot.

Examples

The following example shows how to check and repair an Oracle ACFS file system.

Example 5 Using the `fsck` command

```
# /usr/sbin/fsck -F acfs -y -o a /dev/asm/volume1-123
```

mkfs

Purpose

Creates an Oracle ACFS file system on the Solaris operating system.

Syntax and Description

```
mkfs -F acfs -o h /dev/null
mkfs -F acfs [-o options] volume_device size
```

`mkfs -F acfs -o h /dev/null` displays usage text and exits.

[Table 8](#) contains the options available with the `mkfs` command.

Table 8 Options for the Solaris `mkfs` command

Option	Description
<code>-F acfs</code>	Specifies the type of file system on Solaris. <code>acfs</code> designates the Oracle ACFS type.
<code>-o options</code>	Specifies that options follow (<code>f</code> , <code>h</code> , <code>n</code> , <code>v</code>). Options are preceded with the <code>-o</code> flag and entered as a comma-delimited string. For example: <code>-o f,v</code> <ul style="list-style-type: none"> • <code>h</code> Displays the usage text and exits. • <code>f</code> Specifies the force option. This action creates the file system even if there is an existing Oracle ACFS on the volume device, although only if the file system is dismounted. This option overwrites structures on the original file system. Use this option with caution. • <code>n=name</code> Specifies the name for the file system. A name can be a maximum of 64 characters. <code>acfsutil info fs</code> returns the name if one was specified. • <code>v</code> Specifies verbose mode. The progress is displayed as the operation occurs.
<code>volume_device</code>	Specifies an Oracle ADVM device file.
<code>size</code>	Specifies the size of the file system in 512-byte units or in units of <code>K</code> <code>M</code> <code>G</code> <code>T</code> <code>P</code> . Units specified are in <code>K</code> (kilobytes), <code>M</code> (megabytes), <code>G</code> (gigabytes), <code>T</code> (terabytes), or <code>P</code> (petabytes).

You can use `mkfs` to create the on disk structure needed for Oracle ACFS file system to be mounted. The `mkfs` command is the traditional Linux command used to build a file system. After `mkfs` runs successfully, the `USAGE` column in the `V$ASM_VOLUME` view displays `ACFS`. `root` privilege is not required. The ownership of the volume device file dictates who can run this command.

The minimum file system size is 200 MB.

The Oracle ACFS driver must be loaded for `mkfs` to work.

Examples

Before creating an Oracle ACFS file system, first determine which Oracle ADVM volume devices are available. You can use the `ASMCMD volinfo` command to display information about the volumes and volume devices.

```
ASMCMD [+] > volinfo -a
...
      Volume Name: VOLUME1
      Volume Device: /dev/asm/volume1-123
      State: ENABLED
...
```

See [Managing Oracle ADVM with ASMCMD](#) .

Next create an Oracle ACFS file system on the volume device file.

Example 6 Using the mkfs command

```
$ /usr/sbin/mkfs -F acfs /dev/asm/volume1-123
```

mount**Purpose**

Mounts an Oracle ACFS file system on the Solaris operating system.

Syntax and Description

```
mount -F acfs -o h /tmp /dev/null
mount -F acfs [-r] [-o options] volume_device mount_point
```

`mount -F acfs -o h /tmp /dev/null` displays usage text and exits.

[Table 9](#) contains the options available with the `mount` command.

Table 9 Options for the Solaris mount command

Option	Description
<code>-F acfs</code>	Specifies the type of file system on Solaris. <code>acfs</code> designates the Oracle ACFS type.
<code>-r</code>	Mounts in read-only mode.
<code>-o</code>	Specifies that options follow. Options are preceded with the <code>-o</code> flag followed by a comma-delimited string of options. For example: <code>-o all,v</code> The following options are available: <ul style="list-style-type: none"> • <code>all</code> Reads the Oracle ACFS managed file systems in the Oracle Clusterware namespace, mounting all file systems with the <code>AUTO_START=always</code>. The <code>-o all</code> option requires two placeholders to satisfy the command arguments: a dummy argument for the volume device and any valid directory. When the <code>-o all</code> option is specified, other <code>-o</code> options are ignored. To specify mount options for a registry entry, include those options with the <code>acfsutil registry</code> command when you add the entry to the registry. • <code>devices/nodevices</code> Allows or disallows the opening of any character or block special devices from this mount. • <code>exec/noexec</code> Allows or disallows the execution of programs in this file system. • <code>h</code> Displays the usage help text and exits. • <code>rootsuid/norootsuid</code> Allows or disallows the execution of <code>setuid</code> to root executables (binaries by non-root users whose permissions allow set user Id execution, and are owned by root). <code>rootsuid</code> is the default action. If <code>norootsuid</code> is specified, an attempt to run these executables as a non-root user fails with a permission denied error. • <code>ro</code> Mounts the file system in read-only mode. • <code>rw</code>

Option	Description
	<p>Mounts the file system in read-write mode.</p> <ul style="list-style-type: none"> • <code>setuid/nosetuid</code> Allows or disallows the execution of <code>setuid</code> and <code>setgid</code> programs. • <code>suid/nosuid</code> Allows or disallows the execution of <code>setuid</code> and <code>setgid</code> programs and the opening of any character or block special devices from this mount. • <code>v</code> Specifies verbose mode. The progress is displayed as the operation occurs.
<code>volume_device</code>	Specifies an Oracle ADVM volume device file that has been formatted by <code>mkfs</code> . <code>device</code> is required but can be a dummy value.
<code>mount_point</code>	Specifies the directory where the file system is mounted. This directory must exist before you run the <code>mount</code> command.

`mount` attaches a file system to the Oracle ACFS hierarchy at the mount point that is the name of a directory. The mount occurs on the node where the `mount` command was issued. The `mount` command returns an error if the file system is not in a dismounted state on this node.

It is not always possible to return the cause of a mount failure to the `mount` command. When this happens Oracle ACFS writes the cause of the failure to the system console and associated system log file.

After `mount` runs successfully, the `MOUNTPATH` field in the `V$ASM_VOLUME` view displays the directory name on which the file system is now mounted.

An Oracle ACFS file system should only be mounted on one mount point. The same mount point name should be used on all cluster members.

`root` privilege is required to run `mount`.

Examples

The first example shows how to mount `volume1-123` on the mount point `/acfsmounts/acfs1`. The second example shows how to mount all the registered Oracle ACFS file systems. Placeholder arguments must be provided for the volume device name and mount point when specifying the `-o all` option. The volume device can be a dummy value, such as `none`. Any valid directory can be specified for the mount point, such as `/tmp`.

Example 7 Using the mount command

```
# /sbin/mount -F acfs /dev/asm/volume1-123 /acfsmounts/acfs1
# /sbin/mount -F acfs -o all none /tmp
```

umount/umountall

Purpose

Dismounts an Oracle ACFS file system on the Solaris operating system.

Syntax and Description

```
umount -V [mount_point | volume_device]
umountall -F acfs
```

`umountall -F acfs` dismounts all Oracle ACFS file systems.

[Table 10](#) contains the options available with the `umount` command.

Table 10 Options for the Solaris `umount` command

Option	Description
<code>-V</code>	Echoes the complete command line, but does not run the command. Use this option to verify and validate the command line before execution. Valid only with <code>umount</code> .
<code>mount_point</code>	Specifies the directory where the file system is mounted. Valid only with <code>umount</code> .
<code>volume_device</code>	Specifies the Oracle ADVM volume device name associated with the file system. Valid only with <code>umount</code> .
<code>-F acfs</code>	Specifies the type of file system on Solaris. <code>acfs</code> designates the Oracle ACFS type. Valid only with <code>umountall</code> .

`umount` and `umountall` detach an Oracle ACFS from the file system hierarchy on the current node. If a file system is busy, `umount` and `umountall` fail.

`root` privileges are required to run the `umount` and `umountall` commands.

Examples

The following examples show how to dismount an Oracle ACFS file system. The first example specifies the mount point of the file system to dismount. The second example specifies the volume device associated with the file system to dismount. The third example dismounts all Oracle ACFS file systems.

Example 8 Using the `umount` command

```
# /sbin/umount /dev/asm/volume1-123
# /sbin/umount /acfsmounts/acfs1
# /sbin/umountall -F acfs
```

Oracle ACFS Command-line Tools for the AIX Environment

During the installation of Oracle ACFS and Oracle ADVM with Oracle Grid Infrastructure on AIX, several system security classes (authorizations) are created for Oracle ACFS and Oracle ADVM operations. These authorizations enable the following operations:

- Configuration of Oracle ACFS and Oracle ADVM devices
- Removal of Oracle ACFS and Oracle ADVM devices
- Definition of Oracle ACFS and Oracle ADVM devices

These authorizations are collected in a role (`oracle_devmgmt`) which is assigned by default to the Oracle Grid Infrastructure user and Oracle ASM administrator. You can run the `lsrole` or `roledlist` command after installation to see this new role. These

commands can be run at any time to ensure that the user has the proper authorization to manage Oracle ACFS and Oracle ADVM.

For example, run the following as the Oracle ASM administrator:

```
$ rolelist -e
  oracle_devmgmt
```

After the initial installation on an AIX operating system, the shell from which the root script was run does not inherit the new role. If the role is not present for the user, then the `swrole` command must be run before performing Oracle ACFS or Oracle ADVM operations.

For example, run the following as the Oracle ASM administrator:

```
$ swrole oracle_devmgmt
```

Alternatively, you can open a new shell to perform Oracle ACFS or Oracle ADVM operations.

During the removal of Oracle Grid Infrastructure, the `oracle_devmgmt` role and its associated authorizations are deleted from the system.

See Also:

Oracle Grid Infrastructure on AIX, refer to *Oracle Grid Infrastructure Installation Guide for IBM AIX on POWER Systems (64-Bit)* for more information about installing

Note:

If a disk group is dismounted with the force option on AIX, any Oracle ADVM volumes device files that were on that disk group remain on the system. These files are removed when the disk group is remounted.

[page 16-35](#) contains a summary of the Oracle ACFS commands for the AIX operating system. The commands in [page 16-35](#) have been extended with additional options to support Oracle ACFS on AIX.

Command	Description
fscv	Checks and repairs an Oracle ACFS file system on AIX.
mkfs	Creates an Oracle ACFS file system on AIX.
mount	Mounts an Oracle ACFS file system on AIX.
umount/umountall	Dismounts an Oracle ACFS file system on AIX.

fsck

Purpose

Checks and repairs an Oracle ACFS file system on the AIX operating system.

Syntax and Description

```
fsck -V acfs [-n|-y] [-o options] volume_device
```

Table 12 contains the options available with the AIX `fsck` command.

Table 12 Options for the AIX `fsck` command

Option	Description
<code>-V acfs</code>	Specifies an Oracle ADVM volume on AIX. <code>acfs</code> designates the Oracle ACFS type.
<code>-n</code>	Answers no to any prompts.
<code>-y</code>	Answers yes to any prompts.
<code>-o options</code>	Specifies that options follow (a, f, v). Options are preceded with the <code>-o</code> flag and entered as a comma-delimited string. For example: <code>-o a, v</code> <ul style="list-style-type: none"> • a Specifies to automatically fix the file system. • f Forces the file system into mountable state without completing a file system check or fix. • v Specifies verbose mode. The progress is displayed as the operation occurs. Running in verbose mode can impact performance.
<code>volume_device</code>	Specifies the primary Oracle ADVM volume device.

`fsck` checks and repairs an existing Oracle ACFS. This command can only be run on a dismounted file system. `root` privileges are required to run `fsck`. The Oracle ACFS driver must be loaded for `fsck` to work.

By default, `fsck` only checks for and reports any errors. The `-a` flag must be specified to instruct `fsck` to fix errors in the file system. Do not interrupt `fsck` during the repair operation.

In a few cases, `fsck` prompts for questions before proceeding to check a file system. These cases include:

- If `fsck` detects that another `fsck` is in progress on the file system
- If `fsck` detects that the Oracle ACFS driver is not loaded
- If the file system does not appear to be Oracle ACFS

In checking mode, `fsck` also prompts if there are transaction logs that have not been processed completely due to an incomplete shutdown. To run in a non-interactive mode, include either the `-y` or `-n` options to answer yes or no to any questions.

`fsck` creates working files before it checks a file system. These working files are created in `/usr/tmp` if space is available. `/tmp` is used if `/usr/tmp` does not exist. If insufficient space is available in the `tmp` directory, `fsck` attempts to write to the current working directory. The files that `fsck` creates are roughly the size of the file system being checked divided by 32K. At most three such files are allocated. For example, a 2 GB file system being checked causes `fsck` to generate one to three 64K working files in the `/usr/tmp` directory. These files are deleted after `fsck` has finished.

In the event that `fsck` finds a file or directory in the file system for which it cannot determine its name or intended location (possibly due to a corruption in its parent directory), it places this object in the `/lost+found` directory when `fsck` is run in fix mode. For security reasons only the `root` user on Linux can read files in `/lost`

+found. If the administrator can later determine the original name and location of the file based on its contents, the file can be moved or copied into its intended location.

The file names in the /lost+found directory are in the following formats:

```
parent.id.file.id.time-in-sec-since-1970
parent.id.dir.id.time-in-sec-since-1970
```

The *id* fields are the internal Oracle ACFS numeric identifiers for each file and directory in the file system.

You can use `acfsutil info id id mount_point` to attempt to determine the directory associated with `parent.id`. This directory is assumed to be where the deleted object originated. For information about `acfsutil info`, see “[acfsutil info file](#)”.

If the parent directory is not known, the parent *id* field is set to UNKNOWN.

Note:

It is not possible to see the contents of the /lost+found directory from a snapshot.

Examples

The following example shows how to check and repair an Oracle ACFS file system.

Example 9 Using the fsck command

```
# /usr/sbin/fsck -V acfs -y -o a /dev/asm/volume1-123
```

mkfs

Purpose

Creates an Oracle ACFS file system on the AIX operating system.

Syntax and Description

```
mkfs -V acfs -o h /dev/null
mkfs -V acfs [-v name ] [-s size][-o options] volume_device
```

`mkfs -V acfs -o h /dev/null` displays usage text and exits.

[Table 13](#) contains the options available with the AIX `mkfs` command.

Table 13 Options for the AIX `mkfs` command

Option	Description
<code>-V acfs</code>	Specifies the type of file system on AIX. <code>acfs</code> designates the Oracle ACFS type.
<code>-v name</code>	Specifies the name for the file system. A name can be a maximum of 64 characters. <code>acfsutil info fs</code> returns the name if one was specified.
<code>-s size</code>	Specifies the size of the file system in 512-byte units or in units of K M G T P. Units specified are in K (kilobytes), M (megabytes), G (gigabytes), T (terabytes), or P (petabytes).

Option	Description
<code>-o options</code>	Specifies that options follow (f, h, v). Options are preceded with the <code>-o</code> flag and entered as a comma-delimited string. For example: <code>-o f,v</code> <ul style="list-style-type: none"> • <code>f</code> Specifies the force option. This action creates the file system even if there is an existing Oracle ACFS on the volume device, although only if the file system is dismounted. This option overwrites structures on the original file system. Use this option with caution. • <code>h</code> Displays the usage text and exits. • <code>v</code> Specifies verbose mode. The progress is displayed as the operation occurs.
<code>volume_device</code>	Specifies an Oracle ADVM device file that is to be formatted.

You can use `mkfs` to create the on disk structure needed for Oracle ACFS file system to be mounted. The `mkfs` command is the traditional Linux command used to build a file system. After `mkfs` runs successfully, the `USAGE` column in the `V$ASM_VOLUME` view displays `ACFS`. `root` privilege is not required. The ownership of the volume device file dictates who can run this command.

The minimum file system size is 200 MB.

The Oracle ACFS driver must be loaded for `mkfs` to work.

Examples

Before creating an Oracle ACFS file system, first determine which Oracle ADVM volume devices are available. You can use the `ASMCMD volinfo` command to display information about the volumes and volume devices.

```
ASMCMD [+] > volinfo -a
...
      Volume Name: VOLUME1
      Volume Device: /dev/asm/volume1-123
      State: ENABLED
...
```

See [Managing Oracle ADVM with ASMCMD](#).

Next create an Oracle ACFS file system on the volume device file.

Example 10 Using the `mkfs` command

```
$ /usr/sbin/mkfs -V acfs /dev/asm/volume1-123
```

mount

Purpose

Mounts an Oracle ACFS file system on the AIX operating system.

Syntax and Description

```
mount -V acfs -o h /dev/null /xxx
mount -v acfs [-o options] volume_device mount_point
```

`mount -V acfs -o h /dev/null /xxx` displays usage text and exits.

Table 14 contains the options available with the `mount` command.

Table 14 Options for the AIX mount command

Option	Description
<code>-v acfs</code>	Specifies the type of file system on AIX. <code>acfs</code> designates the Oracle ACFS type.
<code>-o options</code>	<p>Specifies that options follow. Options are preceded with the <code>-o</code> flag followed by a comma-delimited string of options. For example: <code>-o all,ro,v</code></p> <p>The following options are available:</p> <ul style="list-style-type: none"> • <code>all</code> Reads the Oracle ACFS managed file systems in the Oracle Clusterware namespace, mounting all file systems with the <code>AUTO_START=always</code>. The <code>-o all</code> option requires two placeholders to satisfy the command arguments: a dummy argument for the volume device and directory. When the <code>-o all</code> option is specified, other <code>-o</code> options are ignored. To specify mount options for a registry entry, include those options with the <code>acfsutil registry</code> command when you add the entry to the registry. • <code>h</code> Displays the usage help text and exits. • <code>nosuid</code> Specifies that the execution of <code>setuid</code> and <code>setgid</code> programs by way of this mount is not allowed. • <code>nodev</code> Specifies that you cannot open devices from this mount. • <code>norootsuid</code> Fails the execution of binaries by non-root users whose permissions allow set user Id execution, and are owned by root. An attempt to run these executables as a non-root user fails with a permission denied error. • <code>rootsuid</code> Allows the execution of binaries by non-root users of set user Id files owned by root. This is the default action. • <code>ro</code> Mounts the file system in read-only mode. • <code>rw</code> Mounts the file system in read-write mode. • <code>v</code> Specifies verbose mode. The progress is displayed as the operation occurs.
<code>volume_device</code>	Specifies an Oracle ADVM volume device file that has been formatted by <code>mkfs</code> . <code>device</code> is required but can be a dummy value.
<code>mount_point</code>	Specifies the directory where the file system is mounted. This directory must exist before you run the <code>mount</code> command.

`mount` attaches a file system to the Oracle ACFS hierarchy at the mount point that is the name of a directory. The mount happens on the node where the mount command was issued. The mount command returns an error if the file system is not in a dismounted state on this node.

It is not always possible to return the cause of a mount failure to the `mount` command. When this happens Oracle ACFS writes the cause of the failure to the system console and associated system log file.

After `mount` runs successfully, the `MOUNTPATH` field in the `V$ASM_VOLUME` view displays the directory name on which the file system is now mounted.

An Oracle ACFS file system should only be mounted on one mount point. The same mount point name should be used on all cluster members.

`root` privilege is required to run `mount`.

Examples

The first example shows how to mount `volume1-123` on the mount point `/acfsmounts/acfs1`. The second example shows how to mount all the registered Oracle ACFS file systems. The dummy names (`none`) have been entered as placeholders for the device and directory as these arguments are required, but not used, when the `all` option is specified.

Example 11 Using the mount command

```
# /usr/sbin/mount -v acfs /dev/asm/volume1-123 /acfsmounts/acfs1
# /usr/sbin/mount -v acfs -o all none none
```

umount/umountall

Purpose

Dismounts an Oracle ACFS file system on the AIX operating system.

Syntax and Description

```
umount [mount_point | volume_device]
umountall -F acfs
```

`umountall -F acfs` dismounts all Oracle ACFS file systems.

[Table 15](#) contains the options available with the `umount` command.

Table 15 Options for the AIX umount command

Option	Description
<code>mount_point</code>	Specifies the directory where the file system is mounted. Valid only with <code>umount</code> .
<code>volume_device</code>	Specifies the Oracle ADVM volume device name associated with the file system. Valid only with <code>umount</code> .
<code>-F acfs</code>	Specifies the type of file system on AIX. <code>acfs</code> designates the Oracle ACFS type. Valid only with <code>umountall</code> .

`umount` and `umountall` detach an Oracle ACFS from the file system hierarchy on the current node. If a file system is busy, `umount` and `umountall` fail.

`root` privileges are required to run the `umount` and `umountall` commands.

Examples

The following examples show how to dismount an Oracle ACFS file system. The first example specifies the mount point of the file system to dismount. The second example

specifies the volume device associated with the file system to dismount. The third example dismounts all Oracle ACFS file systems.

Example 12 Using the umount command

```
# /usr/sbin/umount /dev/asm/volume1-123

# /usr/sbin/umount /acfsmounts/acfs1

# /usr/sbin/umountall -F acfs
```

Oracle ACFS Command-line Tools for Windows Environments

[page 16-41](#) contains a summary of the Oracle ACFS file system commands for Windows. These commands have been extended to support Oracle ACFS. All other Windows file system commands operate without change for Oracle ACFS.

Command	Description
acfschkdsk	Checks and repairs an Oracle ACFS file system on Windows.
acfsdismount	Dismounts an Oracle ACFS on Windows.
acfsformat	Creates an Oracle ACFS file system on Windows.
acfsmountvol	Mounts an Oracle ACFS file system on Windows.
acfsutil detach	Prepares the Oracle ACFS driver for module unload on Windows.

[page 16-41](#) contains a summary of the non-Oracle ACFS file system commands for Windows.

Command	Description
advmutil dismount	Dismounts Oracle ADVM volume devices for file systems that are not Oracle ACFS on Windows.
advmutil list	Lists Oracle ADVM volume devices for file systems that are not Oracle ACFS on Windows.
advmutil mount	Mounts Oracle ADVM volume devices for file systems that are not Oracle ACFS on Windows.

acfschkdsk

Purpose

Checks and repairs an Oracle ACFS file system.

Syntax and Description

```
acfschkdsk /h
acfschkdsk [/a|/f] [/v] [/n|/y] volume_device
```

[Table 18](#) contains the options available with the `acfschkdsk` command.

Table 18 Options for the acfschkdsk command

Option	Description
/a	Specifies to automatically repair the file system.

Option	Description
/f	Forces the file system into mountable state without completing a file system check or repair.
/v	Specifies verbose mode. The progress is displayed as the operation occurs. Running in verbose mode can impact performance.
/h	Displays the usage help text and exits.
/n	Answers no to any prompts.
/y	Answers yes to any prompts.
<i>volume_device</i>	Specifies the Oracle ADVM volume device.

`acfschkdsk` checks and repairs an existing Oracle ACFS. This command can only be run on a file system that has been dismounted clusterwide.

The Oracle ACFS driver must be loaded for `acfschkdsk` to work. If the driver is not loaded, the administrator is prompted to ensure this is intentional. For information about loading drivers, see [“Oracle ACFS Drivers Resource Management”](#).

The Oracle ACFS driver normally ensures that `acfschkdsk` is the only user of the file system clusterwide. In extreme cases it may be necessary to fix a file system without loading the driver if the file system automount causes the system to fail. The verifications that are normally done by the driver for exclusive access are bypassed in this case.

By default `acfschkdsk` only checks for and only reports errors. The `/a` flag must be specified to instruct `acfschkdsk` to repair errors in the file system. Do not interrupt `acfschkdsk` during the repair operation.

In a few cases, `acfschkdsk` prompts for questions before proceeding to check a file system. For example, if `acfschkdsk` detects that another `acfschkdsk` is in progress on the file system, or if `acfschkdsk` detects that the Oracle ACFS driver is not loaded, or if the file system does not appear to be Oracle ACFS. In checking mode, `acfschkdsk` also prompts if there are transaction logs that have not been processed completely due to an incomplete shutdown. To run in a non-interactive mode, include either the `/y` or `/n` options to answer yes or no to any questions.

`acfschkdsk` creates working files before it checks a file system. These working files are created in the `temp` directory if space is available. If insufficient space is available, `acfschkdsk` attempts to write in the current working directory. The files `acfschkdsk` creates are roughly the size of the file system being checked divided by 32K. At most three files are allocated. These files are deleted when `acfschkdsk` has finished.

In the event that `acfschkdsk` finds a file or directory in the file system for which it cannot determine its name or intended location (possibly due to a corruption in its parent directory), it places this object in the `\lost+found` directory when `acfschkdsk` is run in fix mode. For security reasons, only the Windows Administrator can read files in `\lost+found`. If the administrator can later determine the original name and location of the file based on its contents, the file can be moved or copied into its intended location.

The file names in the `\lost+found` directory are in the following formats:

```
parent.id.file.id.time-in-sec-since-1970
parent.id.dir.id.time-in-sec-since-1970
```

The *id* fields are the internal Oracle ACFS numeric identifiers for each file and directory in the file system.

You can use `acfsutil info id id mount_point` to attempt to determine the directory associated with `parent . id`. This directory is assumed to be where the deleted object originated. For information about `acfsutil info`, see “[acfsutil info file](#)”.

If the parent directory is not known, the parent *id* field is set to UNKNOWN.

Note:

It is not possible to see the contents of the `\lost+found` directory from a snapshot.

Examples

The following example shows how to check an Oracle ACFS file system on Windows.

Example 13 Using the `acfschkdsk` command

```
C:\> acfschkdsk asm-volume1-311
```

acfsdismount

Purpose

Dismounts an Oracle ACFS file system and removes its mount point (name space attachment).

Syntax and Description

```
acfsdismount /h
acfsdismount [/v] {drive_letter | mount_point}
acfsdismount [/v] /all
```

[Table 19](#) contains the options available with the `acfsdismount` command.

Table 19 Options for the `acfsdismount` command

Option	Description
<code>/v</code>	Specifies verbose mode. The progress is displayed as the operation occurs.
<code>/h</code>	Displays help text and exits.
<code>/all</code>	Specifies to dismount all Oracle ACFS file systems on this node.
<code>drive_letter</code>	Specifies the drive letter followed by a colon.
<code>mount_point</code>	Specifies the full path of the mount point including the drive letter.

`acfsdismount` removes the mount point (name space attachment) for the specified file system on the current node and dismounts the file system if it is mounted. When the file system is in the dismounted state, the data is preserved on the device and the file system can be re-mounted with the `acfsmountvol` command.

`acfsdismount` can fail in some circumstances because there are open file references from various programs, such as a virus scanner, Process Explorer, or Oracle Enterprise Manager.

Windows Administrator privileges are required to use the `acfsdismount` command.

Examples

The following examples show how to dismount an Oracle ACFS file system. The first example dismounts a file system using only the drive letter. The second example dismounts a file system using the full path name. The third examples dismounts all mounted file systems. All the examples enable the verbose mode.

Example 14 Using the `acfsdismount` command

```
C:\> acfsdismount /v O:

C:\> acfsdismount /v O:\mnt\

C:\oracle>acfsdismount /v /all
acfsdismount: valid path name: C:\oracle\acfsmounts\acfs1\
acfsdismount: opening handle to volume C:\oracle\acfsmounts\acfs1
acfsdismount: locking volume C:\oracle\acfsmounts\acfs1
acfsdismount: dismounting volume C:\oracle\acfsmounts\acfs1
acfsdismount: removing volume mount point on C:\oracle\acfsmounts\acfs1\
acfsdismount: closing handle to volume C:\oracle\acfsmounts\acfs1 and exiting
cleanly
```

acfsformat

Purpose

Creates an Oracle ACFS file system.

Syntax and Description

```
acfsformat /h
acfsformat [/v] [/f] [/n name] volume_device [blocks]
```

[Table 20](#) contains the options available with the `acfsformat` command.

Table 20 Options for the `acfsformat` command

Option	Description
<code>/v</code>	Specifies verbose mode. The progress is displayed as the operation occurs.
<code>/n name</code>	Specifies the name for the file system. This is also known as a volume label. <code>acfsutil info fs</code> returns the name if one was specified. This can also be displayed from the <code>VOL_LABEL</code> column in the <code>V\$ASM_ACFSVOLUMES</code> view.
<code>/f</code>	Specifies the force option. This action creates the file system even if there is an existing Oracle ACFS on the device, although only if the file system is dismounted. This option overwrites structures on the original file system. Use this option with caution.
<code>/h</code>	Displays the usage help text.
<code>blocks</code>	Specifies the number of blocks that the file system should consume on the named device. The quantity specified can be in units of K (kilobytes), M (megabytes), G (gigabytes), or T

Option	Description
	(terabytes). If a unit is not specified, the default is bytes. If this option is not specified, the entire device is consumed.
<i>volume_device</i>	Specifies an Oracle ADVM device file to be formatted.

`acfsformat` creates the on disk structure needed for Oracle ACFS to be mounted. `acfsformat` performs a quick format on the target volume. After `acfsformat` runs successfully, the `USAGE` column in the `V$ASM_VOLUME` view displays ACFS.

The minimum file system size is 200 MB.

The Oracle ACFS driver must be loaded for `acfsformat` to work.

Windows Administrator privileges are required to run this command.

Examples

This example shows how to create an Oracle ACFS file system. The verbose option is specified in this example.

Example 15 Using the `acfsformat` command

```
C:\> acfsformat /v asm-volume1-311
```

acfsmountvol

Purpose

Mounts an Oracle ACFS file system.

Syntax and Description

```
acfsmountvol /h
acfsmountvol
acfsmountvol [/v] /all
acfsmountvol [/v] { drive_letter | dir } volume_device
```

[Table 21](#) contains the options available with the `acfsmountvol` command.

Table 21 Options for the `acfsmountvol` command

Option	Description
<code>/v</code>	Specifies verbose mode. The progress is displayed as the operation occurs.
<code>/h</code>	Displays the help usage text and exits.
<code>/all</code>	Reads the ACFS mount registry created with <code>acfsutil registry</code> and mounts the file systems listed in it on this node.
<i>drive_letter</i>	The Windows drive letter to link to an Oracle ADVM volume device.
<i>dir</i>	Specifies the full directory of the mount point including the drive letter.
<i>volume_device</i>	Specifies an Oracle ADVM volume device file that has been formatted by <code>acfsformat</code> .

`acfsmountvol` attaches an Oracle ACFS to the file system hierarchy at the specified path name or drive letter. *dir* must be an empty directory. Oracle ACFS mount points can be created on any empty directory and they can be hierarchical (nested).

After `acfsmountvol` runs successfully, the `MOUNTPATH` column in the `V $ASM_VOLUME` view displays the full path or drive letter on which the file system is now mounted. If no arguments are specified, the command lists all mounted Oracle ACFS file systems on this node.

It is not always possible to return the cause of a mount failure to the `acfsmountvol` command. When this happens Oracle ACFS writes the cause of the failure to the Windows system event logger.

An Oracle ACFS file system should only be mounted on one mount point. The same mount point name should be used on all cluster members.

Windows Administrator privileges are required to mount an Oracle ACFS.

Examples

The first example shows how to mount `asm-volume1-311` on the mount point identified as the `F:` drive. The second example shows how to mount `asm-volume1-215` on the mount point specified by `c:\oracle\acfsmounts\acfs1\`. The first two examples enable verbose mode. The third example lists all the mounted file systems on the node.

Example 16 Using the `acfsmountvol` command

```
C:\> acfsmountvol /v F: asm-volume1-215

C:\> acfsmountvol /v c:\oracle\acfsmounts\acfs1 asm-volume1-311

C:\oracle>acfsmountvol
asm-volume1-311
C:\oracle\acfsmounts\acfs1
```

acfsutil detach

Purpose

Prepares the Oracle ACFS driver for module unload.

Syntax and Description

```
acfsutil detach
```

`acfsutil detach` prepares Oracle ACFS for having its driver unloaded. Oracle ACFS registers itself as a base file system upon driver load. In order for the Windows service control manager to send a stop command to the driver, Oracle ACFS must unregister itself as a base file system in addition to deleting any device objects associated with the driver.

After `acfsutil detach` has completed successfully, and all volumes have been dismounted, then the administrator can run the Windows service control manager's stop command to the Oracle ACFS driver. If the `acfsutil detach` command is not used, then the stop command does not call the Oracle ACFS driver unload routine. This command can only be run by the Windows Administrator. It is called automatically by the Oracle ACFS shutdown scripts.

Examples

The following examples show how to detach all Oracle ACFS file systems and unload drivers on Windows. The first example dismounts all the Oracle ACFS file systems volume devices. The second example detaches the volume devices.

Example 17 Using the `acfsutil detach` command

```
C:\> acfsdismount /all
```

```
C:\> acfsutil detach
```

advmutil dismount

Purpose

The `advmutil dismount` command dismounts Oracle ADVM volume devices for file systems that are not Oracle ACFS.

Syntax and Description

```
advmutil dismount [/unregister] {drive_letter | dir}
advmutil dismount [/unregister] [/all | /dg=disk_group]
```

[Table 22](#) contains the options available with the Windows `advmutil dismount` command.

Table 22 Options for the `advmutil dismount` command

Option	Description
<code>drive_letter</code>	Specifies the drive letter to dismount.
<code>dir</code>	Specifies the directory of the mount point, including the drive letter.
<code>/all</code>	Specifies to dismount all file systems on this node.
<code>/unregister</code>	Optionally unregister an Oracle ADVM volume device and its drive letter from the system registry. Upon startup of the Oracle ASM instance and Oracle ACFS, the unregistered drive letter and Oracle ADVM volume symbolic links are not created.
<code>/dg=disk_group</code>	Optional name of the disk group containing the registered Oracle ADVM volume devices to create drive letters or possibly mount or dismount file systems.

Note:

To format an Oracle ADVM volume device with NTFS, it must be mounted on a drive letter. After formatting, Oracle ADVM volume devices with NTFS can be mounted on either a drive letter or a directory.

To successfully run this command, the local Oracle ASM instance must be running and the disk groups required by this command must have been created and mounted in the Oracle ASM instance and volumes enabled.

Examples

These examples show how to dismount a file system that is not Oracle ACFS.

1. The first example shows how to remove a drive letter for an Oracle ADVM volume device which disallows access to the file system.
2. The second example shows how to remove a drive letter for an Oracle ADVM volume device which disallows access to the file system and removes it from the registry.
3. The third example shows how to remove a drive letter for all registered Oracle ADVM volume devices which disallows access to all file systems.
4. The fourth example shows how to remove a drive letter for all registered Oracle ADVM volume devices in a particular Oracle ASM disk group which disallows access to all related file systems.

Example 18 Using the `advmutil dismount` command

```
C:\> advmutil dismount H:
C:\> advmutil dismount H: /unregister
C:\> advmutil dismount /all
C:\> advmutil dismount /dg=data
```

advmutil list

Purpose

The `advmutil list` command lists the Oracle ADVM volume devices that were registered with `advmutil mount /register`.

Syntax and Description

```
advmutil list /registry
```

[Table 23](#) contains the options available with the Windows `advmutil list` command.

Table 23 Options for the `advmutil list` command

Option	Description
<code>list /registry</code>	Lists the drive letter and corresponding Oracle ADVM volume device name contained in the Windows registry.

To successfully run this command, the local Oracle ASM instance must be running and the disk groups required by this command must have been created and mounted in the Oracle ASM instance and volumes enabled.

For information about listing Oracle ADVM volume devices for Oracle ACFS, see "[acfsutil info file](#)".

Examples

The following example shows how to list all entries in the system registry.

Example 19 Using the `advmutil list` command

```
C:\> advmutil list /registry

Drive Letter      Asm Volume
=====
```



```
H:          asm-volume1-123
K:          asm-volume2-245
```

advmutil mount

Purpose

The `advmutil mount` command mounts Oracle ADVM volume devices for file systems that are not Oracle ACFS.

Syntax and Description

```
advmutil mount [/register] {drive_letter | dir} volume_device
advmutil mount /all
```

[Table 24](#) contains the options available with the Windows `advmutil mount` command.

Table 24 Options for the `advmutil mount` command

Option	Description
<code>drive_letter</code>	Specifies the drive letter to mount.
<code>dir</code>	Specifies the directory of the mount point, including the drive letter.
<code>volume_device</code>	Indicates the Oracle ADVM volume device.
<code>/all</code>	Specifies to mount all non-Oracle ACFS file systems on this node.
<code>/register</code>	Optionally register an Oracle ADVM volume device and its drive letter in the Windows system registry. After startup of the Oracle ASM instance and Oracle ACFS, all registered drive letters and Oracle ADVM volume symbolic links are created. This allows for automatic file system mounting by Windows as is also done for Oracle ACFS file systems.

Note:

To format an Oracle ADVM volume device with NTFS, it must be mounted on a drive letter. After formatting, Oracle ADVM volume devices with NTFS can be mounted on either a drive letter or a directory.

To successfully run this command, the local Oracle ASM instance must be running and the disk groups required by this command must have been created and mounted in the Oracle ASM instance and volumes enabled.

For information about registering Oracle ADVM volume devices for Oracle ACFS, see [“acfsutil registry”](#).

Examples

These examples show how to mount a file system that is not Oracle ACFS.

1. The first example shows how to create a drive letter for an Oracle ADVM volume device for use as a non-Oracle ACFS access which you could then use to format the volume for use with NTFS.

2. The second example shows how to create a drive letter for an Oracle ADVM volume device for use as a non-Oracle ACFS access which you could then use to format the volume for use with NTFS and save it in the Windows system registry.
3. The third example shows how to create a drive letter for all Oracle ADVM volume devices which were saved in the system registry which also allows a file system to be accessible.

Example 20 Using the `advmutil mount` command

```
C:\> advmutil mount H: asm-volume1-123
C:\> advmutil mount H: asm-volume1-123 /register
C:\> advmutil mount /all
```

Oracle ACFS Command-Line Tools for Tagging

[Table 25](#) contains a summary of the commands for Oracle ACFS tagging.

You can run `acfsutil help` on all platforms to display help text. You can run `acfsutil version` on all platforms to display the Oracle ACFS version.

When the options are entered with commands on a Windows platform, use `/` instead of `-` with the option. For example, you can display help for `acfsutil` on a Linux platform with `acfsutil -h`. On a Windows platform, use `acfsutil /h`.

A mount point on a Windows operating system can be a drive letter or a directory including the drive letter. When using a drive letter in a command, include the backslash (`\`) with the drive letter, such as in `M:\`, to avoid the possibility of triggering a Windows path substitution to the last accessed path on the specified drive.

On Solaris, `acfsutil tag` commands can set tag names on symbolic link files, but backup and restore utilities do not save the tag names that are explicitly set on the symbolic link files. Also, symbolic link files lose explicitly set tag names if they have been moved, copied, tarred, or paxed.

For an overview of Oracle ACFS tagging, refer to “[Oracle ACFS Tagging](#)”. For information about Oracle ACFS tagging application programming interfaces (APIs), refer to “[Oracle ACFS Tagging Generic Application Programming Interface](#)”.

Table 25 Summary of commands for Oracle ACFS tagging

Command	Description
acfsutil tag info	Displays the tags for directories or files in Oracle ACFS file systems.
acfsutil tag set	Adds a tag to directories or files in an Oracle ACFS file system.
acfsutil tag unset	Removes a tag or all tag names from directories or files in an Oracle ACFS file system.

acfsutil tag info

Purpose

Displays the tag names for tagged directories or file names in Oracle ACFS file systems.

Syntax and Description

```
acfsutil tag info -h
acfsutil tag info [-r] [-c -t tagname] path [path ...]
acfsutil tag info [-c -t tagname]
```

`acfsutil tag info -h` displays help text and exits.

Table 26 contains the options available with the `acfsutil tag info` command.

Table 26 Options for the `acfsutil tag info` command

Option	Description
<code>-t tagname</code>	Specifies the tag name string to display. Enclose the string in quotes if the string contains a space.
<code>path</code>	Specifies the path name to one or more files or directories.
<code>-r</code>	Specifies recursive action on a specified path.
<code>-c</code>	Specifies case-insensitive partial matching on the tag name.

The `acfsutil tag info` command can recursively apply the operation to all child files and subdirectories if the `-r` option is included with specified directory path names.

If no path names are specified, the `acfsutil tag info` command searches all Oracle ACFS mount points for tagged files.

Only the paths of tagged files in an Oracle ACFS file system are displayed. If the `-t tagname` option is included, only paths of files with a tag name exactly matching the specified `tagname` are displayed. If the `-c` option is included, then `tagname` can be a case-insensitive substring of a tag name for a successful match. For example, the `acfsutil tag info -c -t AG` command would display path names of files with tag names such as `tag1`, `ag`, or `AG`.

Any user may use this command to display tag info on a directory that the user has read access privileges.

Running `acfsutil tag info` on a file or directory that is protected by a security realm fails. If a user runs `acfsutil tag info` with the `-r` option on a directory protected by a security realm and the user does not have browse permissions on the directory, then no output is displayed. To resolve this issue, the user must be added to the security realm and granted `READDIR` permissions. For information about adding objects to an Oracle ACFS security realm, refer to “[acfsutil sec realm add](#)”.

Examples

The following example show the use of the `acfsutil tag info` command.

Example 21 Using the `acfsutil tag info` command

```
$ /sbin/acfsutil tag info -r /acfsmounts/acfs1/myrepfiles/
```

acfsutil tag set

Purpose

Adds the given tag to the specified files or directories in an Oracle ACFS file system

Syntax and Description

```
acfsutil tag set -h
acfsutil tag set [-v] [-r] tagname path [path ...]
```

`acfsutil tag set -h` displays help text and exits.

[Table 27](#) contains the options available with the `acfsutil tag set` command.

Table 27 Options for the `acfsutil tag set` command

Option	Description
<i>tagname</i>	Specifies a tag name string. Enclose the string in quotes if the string contains a space. The tag string can be composed of ASCII characters that include: a-b, A-Z, 0-9, the space character, the hyphen, and the underscore. The maximum length of a tag name is 32 characters. <code>all</code> is a reserved tag name and cannot be set on any file or directory.
<i>path</i>	Specifies the path string to one or more files or directories.
<code>-r</code>	Specifies recursive action on the specified path.
<code>-v</code>	Displays the progress of the operation.

The command can recursively apply the operation to all child files and subdirectories for the specified directory path names.

When adding a tag name to a file or directory, the existing tags on that file or directory remain unchanged. New files that are created after a directory is assigned a tag implicitly inherit tags from their parent directories. Existing files in the directory do not inherit the new tag; these files must be explicitly assigned the tag. Renaming a file or moving a file to a subdirectory within the same file system does not cause the file to inherit tag names from the new parent directory. Moving a file between file systems uses a copy operation and the newly created file does inherit the tag names of the parent directory.

There is no fixed maximum number of tag names for an Oracle ACFS file system or for each file and directory. However, the number of tag names is limited by the tag names that fit in up to 64 KB of special metadata storage for each file and directory. This metadata also contains information to manage the extended attributes. Longer tag names reduce the total of tag names that can be set on a file or directory. For example, if all tag names were 4 bytes long, then it is possible to hold approximately 1730 tag names, assuming no other extended attribute information is present.

Any user who has the privilege to modify the target file or directory may run this command.

If a user runs `acfsutil tag set` with the `-r` option on a directory protected by a security realm and does not have browse permissions on the directory, then no tags are applied. To resolve this issue, the user must be added to the security realm and granted `READDIR` permissions. For information about adding objects to an Oracle ACFS security realm, refer to [“acfsutil sec realm add”](#).

Examples

The following example show the use of the `acfsutil tag set` command.

Example 22 Using the `acfsutil tag set` command

```
$ /sbin/acfsutil tag set repl_grpl -r /acfsmounts/acfs1/myrepfiles/*.dat
```

acfsutil tag unset**Purpose**

Removes the given tag name or all tag names from the specified file or directory.

Syntax and Description

```
acfsutil tag unset -h
acfsutil tag unset [-v] [-r] {all | tagname} path [path ...]
```

`acfsutil tag unset -h` displays help text and exits.

[Table 28](#) contains the options available with the `acfsutil tag unset` command.

Table 28 Options for the `acfsutil tag unset` command

Option	Description
<code>all</code>	Specifies to remove all tags in the path string.
<code>tagname</code>	Specifies a tag name string. Enclose the string in quotes if the string contains a space.
<code>path</code>	Specifies the path string to one or more files or directories.
<code>-r</code>	Specifies recursive action on the specified path.
<code>-v</code>	Displays the progress of the operation.

The command can recursively apply the operation to all child files and subdirectories for the specified directory path names.

When removing a tag name from a file or directory, other existing tags on that file or directory remain unchanged.

Any user who has privilege to modify the target file or directory may run this command.

If a user runs `acfsutil tag unset` with the `-r` option on a directory protected by a security realm and does not have browse permissions on the directory, then no tags are removed. To resolve this issue, the user must be added to the security realm and granted `READDIR` permissions. For information about adding objects to an Oracle ACFS security realm, refer to [“acfsutil sec realm add”](#).

Examples

The following example show the use of the `acfsutil tag unset` command.

Example 23 Using the `acfsutil tag unset` command

```
$ /sbin/acfsutil tag unset repl_grpl -r
/acfsmounts/acfs1/myrepfiles/*.log
```

Oracle ACFS Command-Line Tools for Replication

[Table 29](#) contains a summary of the commands for Oracle ACFS replication. For an overview of Oracle ACFS replication, refer to [“Oracle ACFS Replication”](#).

You can run `acfsutil help` on all platforms to display help text. You can run `acfsutil version` on all platforms to display the Oracle ACFS version.

When the options are entered with commands on a Windows platform, use `/` instead of `-` with the option. For example, you can display help for `acfsutil` on a Linux platform with `acfsutil -h`. On a Windows platform, use `acfsutil /h`.

A mount point on a Windows operating system can be a drive letter or a directory including the drive letter. When using a drive letter in a command, include the backslash (`\`) with the drive letter, such as in `M:\`, to avoid the possibility of triggering a Windows path substitution to the last accessed path on the specified drive.

You must use a trailing backslash when specifying a drive letter mount point with replication commands on Windows platforms. For example, use `p:\` (not `p:`) for a drive letter mount point. If the trailing backslash is omitted, this could trigger a Windows path substitution mechanism that replaces the drive letter with the last accessed path on that drive.

Table 29 Summary of commands for Oracle ACFS replication

Command	Description
<code>acfsutil repl bg</code>	Starts, stops, or displays information about the Oracle ACFS replication background processes.
<code>acfsutil repl compare</code>	Verifies that files have been replicated on an Oracle ACFS file system.
<code>acfsutil repl info</code>	Displays information about replication processing on an Oracle ACFS file system.
<code>acfsutil repl init</code>	Initiates replication on files in an Oracle ACFS file system.
<code>acfsutil repl pause</code>	Pauses replication on an Oracle ACFS file system.
<code>acfsutil repl resume</code>	Resumes replication on an Oracle ACFS file system.
<code>acfsutil repl sync</code>	Synchronizes primary and standby file systems.
<code>acfsutil repl terminate</code>	Stops all replication activity on the Oracle ACFS file system.
<code>acfsutil repl trace</code>	Specifies the trace level for replication information.
<code>acfsutil repl update</code>	Updates replication information while replication is running.

acfsutil repl bg

Purpose

Starts, stops, or displays information about the Oracle ACFS replication background processes.

Syntax and Description

```
acfsutil repl bg -h
acfsutil repl bg {start |stop|info} mount_point
```

`acfsutil repl bg -h` displays help text and exits.

[Table 30](#) contains the options available with the `acfsutil repl bg` command.

Table 30 Options for the `acfsutil repl bg` command

Option	Description
<code>start</code>	Starts the replication background processing.
<code>stop</code>	Stops the replication background processing
<code>info</code>	Displays information about the replication background processes.
<code>mount_point</code>	Specifies the directory where the file system is mounted.

Oracle ACFS replication uses background processes to transport file system changes, to communicate between the sites hosting the primary and standby file systems, to monitor the state of replication processing, and to apply file system changes to the standby file system. These background processes must be running for replication to function.

When replication is started with the `acfsutil repl init` command, these background processes are started and are registered with Oracle Clusterware so that they are automatically restarted after a restart or system failure. Usually it is not necessary to run the `acfsutil repl bg` command because Oracle Clusterware automatically starts and stops the background processes as file systems are mounted and unmounted or node membership changes after replication is initialized. However, replication cannot progress if one of the daemons is not running. In this case running `repl bg stop` followed by `repl bg start` ensures that all the daemons are running.

`acfsutil bg start` ensures that all the necessary daemons for replication are running. The daemons may run on different cluster nodes. `acfsutil bg stop` ensures that no daemons for the file system are running on the local node and relocates the daemons to another node if available.

You must have system administrator privileges to run the `acfsutil repl bg start` or `acfsutil repl bg stop` commands. You must have system administrator or Oracle ASM administrator privileges to run the `acfsutil repl bg info` command.

Examples

[Example 24](#) shows the use of the `acfsutil repl bg` command.

Example 24 Using the `acfsutil repl bg` command

```
$ /sbin/acfsutil repl bg start /acfsmounts/acfs1
$ /sbin/acfsutil repl bg stop /acfsmounts/acfs1
$ /sbin/acfsutil repl bg info /acfsmounts/acfs1
```

acfsutil repl compare

Purpose

Verifies that files have been replicated on an Oracle ACFS file system.

Syntax and Description

```
acfsutil repl compare -h
acfsutil repl compare [-a] [-t { all | tagname, ...}]
                        primary_mount_point standby_mount_point
```

`acfsutil repl compare -h` displays help text and exits.

[Table 31](#) contains the options available with the `acfsutil repl compare` command.

Table 31 Options for the `acfsutil repl compare` command

Option	Description
<code>-a</code>	Compares all files and their extended attribute names.
<code>-t {all tagname, ... }</code>	Compares files with all or some tag names specified in the <code>acfsutil repl init</code> operation. The <code>all</code> option specifies all tag names supplied in the <code>acfsutil repl init</code> operation. A comma-delimited list of tag names must only use tag names specified during the <code>acfsutil repl init</code> operation.
<code>primary_mount_point</code>	Specifies the directory where the primary file system is mounted.
<code>standby_mount_point</code>	Specifies the directory where the standby file system is mounted.

The `acfsutil repl compare` command verifies all or part of the primary mount point has been replicated to the standby mount point. The standby mount point must be mounted locally for comparison. Best results are obtained when the primary file system is changing as little as possible.

The `-a` option is typically used when no tag names were specified during the `acfsutil repl init` operation. The `-a` option compares all files on the primary file system against those on the standby file system. The `-a` option also tests for extra files on the standby file system that do not exist on the primary.

The `-t` option is used when tags were specified during the `acfsutil repl init` operation. The `-t` operation locates all file names on the primary file system with the specified tag names and compares them to the corresponding files on the standby. The `-t` option takes as arguments either `all` option or a comma-delimited list of tag names. If the `-t` option is used with `all`, then all tag names supplied during the `acfsutil repl init` operation are selected. Otherwise, any specified tag names must exactly match a tag name supplied during the `acfsutil repl init` operation. The `-t` option also tests for extra files on the standby file system that do not have an associated tag name that was specified during the `acfsutil repl init` operation. You can use the `acfsutil repl info -c` option to determine which tags were specified during the `acfsutil repl init` operation.

If neither the `-a` nor `-t` option is provided, a primary to standby file comparison is done without testing tag names nor extended attributes.

If NFS is used to mount the standby file system locally, the standby cannot be checked for matching tag names and extended attributes due to limitations in the NFS protocol.

Examples

[Example 25](#) shows the use of the `acfsutil repl compare` command.

Example 25 Using the `acfsutil repl compare` command

```
$ /sbin/acfsutil repl compare /acfsmounts/acfs1 /nfs_mounted_standby
```

acfsutil repl info

Purpose

Displays information about replication processing on an Oracle ACFS file system.

Syntax and Description

```
acfsutil repl info -h
acfsutil repl info -c [-v] mount_point
acfsutil repl info -s [-v][-l] [-n number{m|h|d|w|y}]
    [-r start_time[#stop_time]] {-f eventlog | mount_point}
acfsutil repl info [-a|-e|-t] [-v][-l]
    [-r start_time[#stop_time]] {-f eventlog | mount_point }
```

acfsutil repl info -h displays help text and exits.

Table 32 contains the options available with the acfsutil repl info command.

Table 32 Options for the acfsutil repl info command

Option	Description
-a	Displays only apply records from the replication event log. An apply record contains the date and time that the set of file system changes were captured on the primary file system and the date and time that they were applied on the standby file system.
-c	Displays configuration information.
-e	Displays only error records from the replication event log.
-f eventlog	Specifies the absolute path to the replication event log to be used as the source of the information. The default location is: <code>mount_point/.ACFS/repl/logs/ReplicationEventsLog</code>
-h	Displays help text.
-l	Displays last event only.
-n number{m h d w y}	Specifies the interval to display information. <i>number</i> specifies the number of minutes (m), hours (h), days (d), weeks (w), or years (y). For example: <code>-n 5d</code> The statistics are summarized in the units of time specified.
-r start_time[#stop_time]]	Specifies the start and stop time to display information. The format for the time period is <code>yyyy-nn-ddThh:mm:ss</code> . yyyy - year nn - month (01..12) dd - day (01..31) hh - hour (00..23) mm - minute (00..59) ss - second (00..59) For example: <code>-r 2010-05-05T08:30:00#2010-05-05T15:30:00</code>
-s	Displays statistical information. This option is valid only when run on the primary file system. It is important that the primary and standby nodes are running a network time service to ensure that the statistics are meaningful.
-t	Displays only transport records from the replication event log.
-v	Displays verbose output.
mount_point	Specifies the directory where the file system is mounted.

To display information about replication configuration, use `acfsutil repl info` with the `-c` option. The configuration information includes a Last sync time with

primary timestamp that identifies the point in time on the primary file system that the standby file system represents. You can use this timestamp to set back a database to this point in time if it is necessary to keep the data in Oracle ACFS file system synchronized with the database data replicated with Oracle Data Guard.

To display information about replication statistics, use `acfsutil repl info` with the `-s` option.

To display information about replication events, use `acfsutil repl info` with the `-a`, `-e`, or `-t` options.

You must have system administrator or Oracle ASM administrator privileges to run this command.

Examples

[Example 26](#) shows the use of the `acfsutil repl info` command.

Example 26 Using the `acfsutil repl info` command

```
$ /sbin/acfsutil repl info -c /acfsmounts/acfs1
$ /sbin/acfsutil repl info -s -n 5d /acfsmounts/acfs1
$ /sbin/acfsutil repl info -a -v /acfsmounts/acfs1
```

acfsutil repl init

Purpose

Initiates replication on all the files in an Oracle ACFS file system or only those files with a specified list of tags.

Syntax and Description

```
acfsutil repl init -h
acfsutil repl init primary -s standby_connect_string [tagname...]
    [-m standby_mount_point] [-c primary_service]
    [-d trace_level] [-z {on|off}] mount_point
acfsutil repl init standby -p primary_connect_string
    [-c standby_service] [-d trace_level] mount_point
```

`acfsutil repl init -h` displays help text and exits.

[Table 33](#) contains the options available with the `acfsutil repl init` command.

Table 33 Options for the `acfsutil repl init` command

Option	Description
<code>primary</code>	Specifies replication of the primary file system.
<code>standby</code>	Specifies replication of the standby file system.
<code>-s</code> <code><i>standby_connect_string</i></code>	Specifies the connection string for the site hosting the standby file system. The user in the connection string must have SYSASM and SYSDBA privileges. Oracle wallets should be used to manage security credentials.
<code>-p</code> <code><i>primary_connect_string</i></code>	Specifies the connection string for the site hosting the primary file system. The user in the connection string must have SYSASM and SYSDBA privileges. Oracle wallets should be used to manage security credentials.

Option	Description
<i>tagname</i>	Specifies the tag names of the files to be replicated.
-m <i>standby_mount_point</i>	Specifies the directory where the standby file system is mounted if it is different than the primary file system. This is valid only for the primary file system initialization.
-c <i>primary_service</i>	Specifies the service name for the primary file system. Required if the primary file system is using a different service name than the standby file system.
-c <i>standby_service</i>	Specifies the service name for the standby file system. Required if the standby file system is using a different service name than the primary file system.
-d <i>trace_level</i>	Specifies the trace level setting (0..6) for replication logs.
-z on off	Turn on or off compression on replication logs. Compression is off by default.
<i>mount_point</i>	Specifies the directory where the file system is mounted. For <code>repl init primary</code> , <i>mount_point</i> specifies the primary file system. For <code>repl init standby</code> , <i>mount_point</i> specifies the standby file system.

When the `acfsutil repl init primary` command completes successfully, processing begins to replicate initial copies of all specified files to the standby file system. In addition, any changes to these files and any new files subsequently created in the file system on the primary file system are captured and transported to the standby file system. However, successful completion of the command does not indicate that the specified files have been copied in full to the standby file system. To monitor the progress of the initial replication of all specified files to the standby file system, users run the `acfsutil repl info -c` command.

The first phase of the initial replication copy process begins with a complete copy of the file system directory tree structure, not the files within the directory tree, to the standby file system. This copy process includes directories without specified tags. During the copy process, attempts to rename directories may fail. After the directory tree structure has been successfully copied to the standby file system, replication initialization begins the second phase of the initial copy process: copying all files to be replicated to the standby file system. While a file is being copied to the standby file system during this initial replication phase, writes and truncates to that file are blocked.

Symbolic link files are replicated as is. If the symbolic link resolves to an absolute path name, and that path name does not exist on the standby file system, then referencing the symbolic link results in errors.

A new service name must be created for replication. You cannot use the +ASM service name. You must specify a unique service name for each file system that you want to replicate when there are multiple replicated file systems on a node or cluster.

A file system being replicated can only be mounted on one path for the primary or standby file system. Otherwise, dismounting any path on a node where it is mounted on multiple paths stops the replication background threads.

A replicated Oracle ACFS file system must be mounted on the same directory within a cluster. The file system does not have to be mounted on all of the nodes in a cluster, but if it is mounted, it must be mounted on the directory specified with the `acfsutil repl init` command. In addition, no other file system can be mounted on that directory on other nodes.

A single Oracle ACFS file system cannot be configured both as a primary and a standby file system. If replication is configured on the same host or within the same cluster, then the primary and standby file systems cannot use the same named mount point.

The primary file system must have a minimum size of 4 GB for each node that is mounting the file system. The standby file system must have a minimum size of 4 GB and should be sized appropriately for the amount of data being replicated and the space necessary for the replication logs sent from the primary file system.

The sites hosting the primary and standby file systems must be running the same operating system and must have the same system architecture.

Oracle wallets should be used to manage security credentials.

See Also:

- *Oracle Database Enterprise User Security Administrator's Guide* for information about Oracle wallets
 - *Oracle Database SecureFiles and Large Objects Developer's Guide* for information about wallet management
 - *Oracle Database Net Services Reference* for information about wallet parameters in the `SQLNET.ORA` file
-
-

You must have system administrator privileges to run this command.

Examples

[Example 27](#) shows the use of the `acfsutil repl init` command to set up the primary and standby file systems. In these examples, the connect string searches in the user's wallet for the user name and password associated with the alias `primary_repl_site` or `standby_repl_site`.

Example 27 Using the `acfsutil repl init` command

```
$ /sbin/acfsutil repl init primary
-s /@standby_repl_site
-m /standby/repl_data -c primary_repl_service
/acfsmounts/repl_data

$ /sbin/acfsutil repl init standby
-p /@primary_repl_site
-c standby_repl_service /standby/repl_data
```

acfsutil repl pause

Purpose

Pauses replication on an Oracle ACFS file system.

Syntax and Description

```
acfsutil repl pause -h
acfsutil repl pause mount_point
```

`acfsutil repl pause -h` displays help text and exits.

Table 34 contains the options available with the `acfsutil repl pause` command.

Table 34 Options for the `acfsutil repl pause` command

Option	Description
<code>mount_point</code>	Specifies the directory where the file system is mounted.

The `acfsutil repl pause` command temporarily stops the replication process until the `acfsutil repl resume` command is run. The command can be run at either the site hosting the primary or a standby file system. `acfsutil repl resume` should be run soon after `acfsutil repl pause` to resume replication.

You can use the `acfsutil repl pause` command to temporarily stop the transportation of replication logs from the primary file system to the standby file system, but logs continue to be generated on the primary file system. Logs are not deleted until they are transported to the standby file system and applied to the standby file system.

The `acfsutil repl pause` command can also be used to temporarily stop the application of replication logs to a standby file system, but the command does not stop the transportation of logs to the standby file system. Logs are not deleted from the standby file system until they are applied to the file system.

When replication is paused on either the site hosting the primary or standby file system, replication logs still accumulate on the standby and primary file system. These logs can consume all available storage space in the file system so you must check available storage on the sites hosting the file systems if you have paused replication. Ensure that you run `acfsutil repl resume` before the accumulated replication logs consume all available space in the file system.

You must have system administrator or Oracle ASM administrator privileges to run this command.

Examples

Example 28 shows the use of the `acfsutil repl pause` command.

Example 28 Using the `acfsutil repl pause` command

```
$ /sbin/acfsutil repl pause /acfsmounts/acfs1
```

acfsutil repl resume

Purpose

Resumes replication on an Oracle ACFS file system where replication has been paused.

Syntax and Description

```
acfsutil repl resume -h
acfsutil repl resume mount_point
```

`acfsutil repl resume -h` displays help text and exits.

Table 35 contains the options available with the `acfsutil repl resume` command.

Table 35 Options for the `acfsutil repl resume` command

Option	Description
<code>mount_point</code>	Specifies the directory where the file system is mounted.

This command resumes the replication process after the `acfsutil repl pause` command has been run. This command should be run soon after replication has been paused with the `acfsutil repl pause` command.

You must have system administrator or Oracle ASM administrator privileges to run this command.

Examples

[Example 29](#) shows the use of the `acfsutil repl resume` command.

Example 29 Using the `acfsutil repl resume` command

```
$ /sbin/acfsutil repl resume /acfsmounts/acfs1
```

acfsutil repl sync

Purpose

Synchronizes primary and standby file systems.

Syntax and Description

```
acfsutil repl sync -h
acfsutil repl sync [apply] mount_point
```

`acfsutil repl sync -h` displays help text and exits.

[Table 36](#) contains the options available with the `acfsutil repl sync` command.

Table 36 Options for the `acfsutil repl sync` command

Option	Description
<code>apply</code>	Specifies that all changes be applied to the standby file system.
<code>mount_point</code>	Specifies the directory where the primary file system is mounted.

You can use the `acfsutil repl sync` command to synchronize the state of the primary and standby file system. This command can only be run on the site hosting the primary file system.

You should first quiesce your applications and run a `sync(1)` call so that the synchronized state is known and meaningful to you. The `acfsutil repl sync` command then causes all outstanding replication data to be shipped from the primary to the standby file system.

The `acfsutil repl sync` command returns success when this transfer is complete or, if the `apply` parameter is supplied, when all of these changes have been successfully applied to the standby file system. At this point, unless an unmount of the last node on the primary site cluster is about to occur, applications can be restarted. You can use the `acfsutil repl sync` command before dismounting the file system on the last node to ensure that all modifications have been sent to the standby file system.

If `acfsutil repl info -c` reports the primary file system is in the `Initializing` state, the `acfsutil repl sync` command does not guarantee that all files to be replicated in the file system have been sent to the standby file system. Files that existed in the file system before running the `acfsutil repl init` command are sent to the standby file system in the background.

You must have system administrator or Oracle ASM administrator privileges to run this command.

Examples

[Example 30](#) shows the use of the `acfsutil repl sync` command.

Example 30 Using the `acfsutil repl sync` command

```
$ /sbin/acfsutil repl sync /acfsmounts/acfs1
```

acfsutil repl terminate

Purpose

Stops all replication activity on the Oracle ACFS file system at the site where it is run.

Syntax and Description

```
acfsutil repl terminate -h
acfsutil repl terminate primary mount_point
acfsutil repl terminate standby [immediate] mount_point
```

`acfsutil repl terminate -h` displays help text and exits.

[Table 37](#) contains the options available with the `acfsutil repl terminate` command.

Table 37 Options for the `acfsutil repl terminate` command

Option	Description
<code>primary</code>	Stops replication on the primary file system.
<code>standby</code>	Stops replication on the standby file system.
<code>immediate</code>	Stops replication processing immediately on the standby file system.
<code>mount_point</code>	Specifies the directory where the file system is mounted.

The `acfsutil repl terminate` command stops all replication processing. When terminating replication, you should terminate replication for the primary file system first, and then the standby file system. If you want to ensure all changes are sent to the standby file system before terminating the primary site, ensure that all applications are quiesced and run the `acfsutil repl sync` command. The `terminate` command must be run on both sites if both sites hosting the file systems are available.

After `acfsutil repl terminate standby` has been run, you can use the standby file system in read-write mode. After `acfsutil repl terminate` has been run on either the primary file system or standby file system, you must start replication from the beginning with the `acfsutil repl init` command.

The `repl terminate standby` command waits until replication data at the standby file system has been applied. If you want to terminate replication immediately without

applying all the replication data, use the `immediate` option. However, this option can leave some files at the standby file system in an indeterminate state.

To momentarily stop Oracle ACFS replication, you can use the `acfsutil repl pause` command, followed soon after by the `acfsutil repl resume` command.

You must have system administrator privileges to run this command.

Examples

[Example 31](#) shows the use of the `acfsutil repl terminate` command.

Example 31 Using the `acfsutil repl terminate` command

```
$ /sbin/acfsutil repl terminate /acfsmounts/acfs1
```

acfsutil repl trace

Purpose

Sets the replication trace level for gathering trace information on an Oracle ACFS file system.

Syntax and Description

```
acfsutil repl trace -h
acfsutil repl trace level mount_point
```

`acfsutil repl trace -h` displays help text and exits.

[Table 39](#) contains the options available with the `acfsutil repl trace` command.

Table 38 Options for the `acfsutil repl trace` command

Option	Description
<code>level</code>	Specifies the trace level setting (0..6). The default level is 2.
<code>mount_point</code>	Specifies the directory where the file system is mounted.

Increasing the trace level can have a performance impact and should be done at the recommendation of Oracle support services.

Trace files for Oracle ACFS replication are stored in the following locations:

```
GRID_HOME/log/hostname/acfsrepl*
GRID_HOME/log/hostname/client/acfsutil.log
```

You must have system administrator or Oracle ASM administrator privileges to run this command.

Examples

[Example 32](#) shows the use of the `acfsutil repl trace` command.

Example 32 Using the `acfsutil repl trace` command

```
$ /sbin/acfsutil repl trace 5 /acfsmounts/acfs1
```

acfsutil repl update

Purpose

Updates replication information while replication is running on an Oracle ACFS file system.

Syntax and Description

```
acfsutil repl update -h
acfsutil repl update [-p primary_connect_string ]
                    [-s standby_connect_string] [-z {on|off}] mount_point
```

`acfsutil repl update -h` displays help text and exits.

[Table 39](#) contains the options available with the `acfsutil repl update` command.

Table 39 Options for the `acfsutil repl update` command

Option	Description
<code>-p</code> <i>primary_connect_string</i>	Specifies the connection string for the primary file system. The user in the connection string must have SYSASM and SYSDBA privileges.
<code>-s</code> <i>standby_connect_string</i>	Specifies the connection string for the standby file system. The user in the connection string must have SYSASM and SYSDBA privileges.
<code>-z on off</code>	Turn on or off compression on replication logs. Compression is off by default.
<i>mount_point</i>	Specifies the directory where the primary file system is mounted.

The `acfsutil repl update` command updates replication information after replication has been started. This command can only be run on the site hosting the primary file system. The connection strings for the primary and standby file systems can be altered.

You can specify any combination of the `-p`, `-s`, and `-z` options, but you must specify at least one of those options.

While replication is running, compression can be turned on or off with the `-z` option.

You must have system administrator privileges to run this command.

Examples

[Example 33](#) shows the use of the `acfsutil repl update` command.

Example 33 Using the `acfsutil repl update` command

```
$ /sbin/acfsutil repl update -s mystandby@oracle.com /acfsmounts/acfs1
```

Oracle ACFS Command-Line Tools for Auditing

[Table 40](#) contains a summary of the commands for Oracle ACFS auditing. For an overview of Oracle ACFS auditing, refer to “[Oracle ACFS Auditing](#)”.

You can run `acfsutil help` on all platforms to display help text. You can run `acfsutil version` on all platforms to display the Oracle ACFS version.

When the options are entered with commands on a Windows platform, use `/` instead of `-` with the option. For example, you can display help for `acfsutil` on a Linux platform with `acfsutil -h`. On a Windows platform, use `acfsutil /h`.

A mount point on a Windows operating system can be a drive letter or a directory including the drive letter. When using a drive letter in a command, include the backslash (\) with the drive letter, such as in M:\, to avoid the possibility of triggering a Windows path substitution to the last accessed path on the specified drive.

Table 40 Summary of commands for Oracle ACFS auditing

Command	Description
<code>acfsutil audit archive</code>	Forces an archival of the audit trail.
<code>acfsutil audit disable</code>	Disables auditing for Oracle ACFS encryption or security.
<code>acfsutil audit enable</code>	Enables auditing for Oracle ACFS encryption or security.
<code>acfsutil audit info</code>	Displays auditing information.
<code>acfsutil audit init</code>	Initializes auditing on an Oracle ACFS environment.
<code>acfsutil audit purge</code>	Purges the audit trail for a specified file system.
<code>acfsutil audit read</code>	Marks the audit trail to indicate that the audit trail has been read.

acfsutil audit archive

Purpose

Forces an archival of the audit trail for the current host on the specified Oracle ACFS file system.

Syntax and Description

```
acfsutil audit archive -h
acfsutil audit archive -m mount_point
```

`acfsutil audit archive -h` displays help text and exits.

[Table 41](#) contains the options available with the `acfsutil audit archive` command.

Table 41 Options for the acfsutil audit archive command

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.

You can use the `acfsutil audit archive` command to safely back up or remove audit data without the possibility of losing intermediate audit messages.

Only an audit manager can run this command.

Examples

The following example shows the use of the `acfsutil audit archive` command.

Example 34 Using the acfsutil audit archive command

```
$ /sbin/acfsutil audit archive -m /acfsmounts/acfs1
```

acfsutil audit disable

Purpose

Disables auditing for either Oracle ACFS encryption or security on a specified file system.

Syntax and Description

```
acfsutil audit disable -h
acfsutil audit disable -m mount_point -s {encr |sec}
```

`acfsutil audit disable -h` displays help text and exits.

[Table 42](#) contains the options available with the `acfsutil audit disable` command.

Table 42 Options for the `acfsutil audit disable` command

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.
<code>-s {encr sec}</code>	Specifies whether to disable auditing for encryption or security.

Only an audit manager can run this command.

Examples

The following example shows the use of the `acfsutil audit disable` command.

Example 35 Using the `acfsutil audit disable` command

```
$ /sbin/acfsutil audit disable -m /acfsmounts/acfs1 -s encr
```

acfsutil audit enable

Purpose

Enables auditing for either Oracle ACFS encryption or security on a specified file system.

Syntax and Description

```
acfsutil audit enable -h
acfsutil audit enable -m mount_point -s {encr |sec}
```

`acfsutil audit enable -h` displays help text and exits.

[Table 43](#) contains the options available with the `acfsutil audit enable` command.

Table 43 Options for the `acfsutil audit enable` command

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.
<code>-s {encr sec}</code>	Specifies whether to enable auditing for encryption or security.

The `acfsutil audit enable` command may also create the `mount_point/.Security/audit` directory, which is a location for audit source

files. The audit directory is created when auditing first is enabled for a file system, as a result of either the `acfsutil encr set`, `acfsutil sec prepare`, or `acfsutil audit enable` command.

Only an audit manager can run this command.

Examples

The following example shows the use of the `acfsutil audit enable` command.

Example 36 Using the `acfsutil audit enable` command

```
$ /sbin/acfsutil audit enable -m /acfsmounts/acfs1 -s encr
```

acfsutil audit info

Purpose

Displays auditing information.

Syntax and Description

```
acfsutil audit info -h  
acfsutil audit info [-m mount_point ]
```

`acfsutil audit info -h` displays help text and exits.

[Table 44](#) contains the options available with the `acfsutil audit info` command.

Table 44 Options for the `acfsutil audit info` command

Option	Description
<code>-m <i>mount_point</i></code>	Optionally specifies the directory where the file system is mounted.

Only an audit manager can run this command.

Examples

The following example shows the use of the `acfsutil audit info` command.

Example 37 Using the `acfsutil audit info` command

```
$ /sbin/acfsutil audit info -m /acfsmounts/acfs1
```

```
Auditing information for '/acfsmounts/acfs1':  
Audit trail size: 10MB  
Archive File: READ  
Audit Sources:  
Security: ENABLED  
Encryption: ENABLED
```

acfsutil audit init

Purpose

Initializes Oracle ACFS auditing.

Syntax and Description

```
acfsutil audit init -h
acfsutil audit init -M audit_manager_group -A auditor_group
```

`acfsutil audit init -h` displays help text and exits.

[Table 45](#) contains the options available with the `acfsutil audit init` command.

Table 45 Options for the `acfsutil audit init` command

Option	Description
<code>-M</code> <code><i>audit_manager_group</i></code>	Specifies the operating system (OS) group which assigns users to the Oracle ACFS audit manager role. To achieve separation of duties, you should create a new group specifically for this purpose and this group should be different from the system administrator group, Oracle ACFS security administrator OS group, and the Oracle ACFS audit auditor OS group.
<code>-A</code> <code><i>auditor_group</i></code>	Specifies the operating system (OS) group which assigns users to the Oracle ACFS audit auditor role. To achieve separation of duties, you should create a new group specifically for this purpose and this group should be different from the system administrator group, Oracle ACFS security administrator OS group, and the Oracle ACFS audit manager OS group.

The `acfsutil audit init` command must be run by the system administrator before enabling auditing for any of the audit sources on a file system. The command sets up the required roles for auditing and must be run before any type of auditing can be enabled on a file system. After running the command, auditing is enabled by default for all features which use auditing.

Because you cannot choose a different OS group for either the Oracle ACFS audit manager or auditor after initialization, you should create new OS groups for these specific purposes before initializing Oracle ACFS auditing.

Only a system administrator can run this command.

Examples

The following example shows the use of the `acfsutil audit init` command.

Example 38 Using the `acfsutil audit init` command

```
# /sbin/acfsutil audit init -M myaudit_mgr_grp -A myauditor_grp
```

acfsutil audit purge

Purpose

Purges the audit trail for a specified file system.

Syntax and Description

```
acfsutil audit purge -h
acfsutil audit purge -m mount_point [-f]
```

`acfsutil audit purge -h` displays help text and exits.

[Table 46](#) contains the options available with the `acfsutil audit purge` command.

Table 46 Options for the acfsutil audit purge command

Option	Description
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-f</code>	Forces the removal of the audit trail even if the audit auditor has not marked the file as read using the <code>acfsutil audit read</code> command.

Only an audit manager can run this command.

Examples

The following example shows the use of the `acfsutil audit purge` command.

Example 39 Using the acfsutil audit purge command

```
$ /sbin/acfsutil audit purge -m /acfsmounts/acfs1 -f
```

acfsutil audit read

Purpose

Marks the audit trail to indicate to the audit manager that the log archive file for the current node has been reviewed, backed up as necessary, and is safe to purge.

Syntax and Description

```
acfsutil audit read -h
acfsutil audit read -m mount_point
```

`acfsutil audit read -h` displays help text and exits.

[Table 47](#) contains the options available with the `acfsutil audit read` command.

Table 47 Options for the acfsutil audit read command

Option	Description
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.

Only an audit auditor can run this command.

Examples

The following example shows the use of the `acfsutil audit read` command.

Example 40 Using the acfsutil audit read command

```
$ /sbin/acfsutil audit read -m /acfsmounts/acfs1
```

Oracle ACFS Command-Line Tools for Security

[Table 48](#) contains a summary of the commands for Oracle ACFS security. For an overview of Oracle ACFS security, refer to "[Oracle ACFS Security](#)".

You can run `acfsutil help` on all platforms to display help text. You can run `acfsutil version` on all platforms to display the Oracle ACFS version.

When the options are entered with commands on a Windows platform, use / instead of - with the option. For example, you can display help for `acfsutil` on a Linux platform with `acfsutil -h`. On a Windows platform, use `acfsutil /h`.

A mount point on a Windows operating system can be a drive letter or a directory including the drive letter. When using a drive letter in a command, include the backslash (\) with the drive letter, such as in `M:\`, to avoid the possibility of triggering a Windows path substitution to the last accessed path on the specified drive.

Table 48 Summary of commands for Oracle ACFS security

Command	Description
<code>acfsutil sec admin add</code>	Adds a security administrator.
<code>acfsutil sec admin password</code>	Changes the password of a security administrator.
<code>acfsutil sec admin remove</code>	Removes a security administrator.
<code>acfsutil sec batch</code>	Runs a batch file.
<code>acfsutil sec disable</code>	Disables Oracle ACFS security.
<code>acfsutil sec enable</code>	Enables Oracle ACFS security.
<code>acfsutil sec info</code>	Displays Oracle ACFS file system security information.
<code>acfsutil sec info file</code>	Lists the security realms that a specified file or directory belongs to.
<code>acfsutil sec init</code>	Initializes Oracle ACFS file system security.
<code>acfsutil sec load</code>	Loads Oracle ACFS file system security metadata.
<code>acfsutil sec prepare</code>	Prepares an Oracle ACFS file system for security.
<code>acfsutil sec realm add</code>	Adds objects to an Oracle ACFS file system security realm.
<code>acfsutil sec realm audit disable</code>	Disables auditing of command rules for files in an Oracle ACFS security realm.
<code>acfsutil sec realm audit enable</code>	Enables auditing of command rules for files in an Oracle ACFS security realm.
<code>acfsutil sec realm audit info</code>	Displays the realm auditing information for a specified Oracle ACFS security realm.
<code>acfsutil sec realm clone</code>	Clones an Oracle ACFS file system security realm.
<code>acfsutil sec realm create</code>	Creates an Oracle ACFS file system security realm.
<code>acfsutil sec realm delete</code>	Removes objects from an Oracle ACFS file system security realm.
<code>acfsutil sec realm destroy</code>	Removes an Oracle ACFS file system security realm.
<code>acfsutil sec rule clone</code>	Clones an Oracle ACFS file system security rule.
<code>acfsutil sec rule create</code>	Creates an Oracle ACFS file system security rule.
<code>acfsutil sec rule destroy</code>	Removes an Oracle ACFS file system security rule.
<code>acfsutil sec rule edit</code>	Updates an Oracle ACFS file system security rule.
<code>acfsutil sec ruleset clone</code>	Clones an Oracle ACFS file system security rule set.
<code>acfsutil sec ruleset create</code>	Creates an Oracle ACFS file system security rule set.
<code>acfsutil sec ruleset destroy</code>	Removes an Oracle ACFS file system rule set.

Command	Description
acfsutil sec ruleset edit	Updates an Oracle ACFS file system rule set.
acfsutil sec save	Saves Oracle ACFS file system security metadata.

acfsutil sec admin add

Purpose

Adds a new security administrator for an Oracle ACFS file system.

Syntax and Description

```
acfsutil sec admin add -h
acfsutil sec admin add admin
```

`acfsutil sec admin add -h` displays help text and exits.

[Table 49](#) contains the options available with the `acfsutil sec admin add` command.

Table 49 Options for the `acfsutil sec admin add` command

Option	Description
<i>admin</i>	Specifies a security administrator user name. The user specified must be an existing operating system user and a member of the security group specified with the <code>acfsutil sec init</code> command. On Windows, a security administrator user name must be specified with a fully qualified domain user name in the form of <i>domain_name\username</i> .

Security administrators are common for all Oracle ACFS file systems in a cluster. A temporary password must be provided for the new security administrator. The password must conform to the format that is described in "[acfsutil sec init](#)".

The new security administrator can change the password with the `acfsutil sec admin password` command. For information, refer to "[acfsutil sec admin password](#)".

Security administrators are allowed to browse all directories in an Oracle ACFS file system whether they have the underlying operating system permissions and whether any realm checks allow it. This exception enables a security administrator to check the location of the files when securing them with Oracle ACFS security realms. However, a security administrator cannot view the contents of individual files without the appropriate operating system and security realm permissions.

Only an existing security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec admin add` command.

Example 41 Using the `acfsutil sec admin add` command

```
$ /sbin/acfsutil sec admin add sec_admin_three
```


acfsutil sec admin password

Purpose

Changes the password of a security administrator for an Oracle ACFS file system.

Syntax and Description

```
acfsutil sec admin password -h
acfsutil sec admin password
```

`acfsutil sec admin password -h` displays help text and exits.

The `acfsutil sec admin password` command changes the security password for the administrator that is running the command. When you run this command, you are prompted to enter a new password. The password must conform to the format that is described in “[acfsutil sec init](#)”.

Every time a security administrator runs an `acfsutil sec` command, the administrator is prompted for the security administrator's password.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec admin password` command.

Example 42 Using the acfsutil sec admin password command

```
$ /sbin/acfsutil sec admin password
ACFS Security administrator password:
New password:
Re-enter new password:
```

acfsutil sec admin remove

Purpose

Removes a security administrator from an Oracle ACFS file system.

Syntax and Description

```
acfsutil sec admin remove -h
acfsutil sec admin remove admin
```

`acfsutil sec admin remove -h` displays help text and exits.

[Table 50](#) contains the options available with the `acfsutil sec admin remove` command.

Table 50 Options for the acfsutil sec admin remove command

Option	Description
<i>admin</i>	Specifies an existing security administrator user name. On Windows, the security administrator user name must be specified with a fully qualified user name in the form of <i>domain_name\username</i> .

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec admin remove` command.

Example 43 Using the `acfsutil sec admin remove` command

```
$ /sbin/acfsutil sec admin remove sec_admin_three
```

acfsutil sec batch

Purpose

Runs a specified batch file.

Syntax and Description

```
acfsutil sec batch -h
acfsutil sec batch batch_file
```

`acfsutil sec batch -h` displays help text and exits.

[Table 51](#) contains the options available with the `acfsutil sec batch` command.

Table 51 Options for the `acfsutil sec batch` command

Option	Description
<i>batch_file</i>	Specifies an existing batch file name. The batch file contains a list of <code>acfsutil sec</code> commands.

The batch file can only contain security realm management commands. Interactive commands are not recommended. The `acfsutil sec admin add`, `acfsutil sec admin password`, and `acfsutil sec init` commands are not supported in the batch file. Also, other `acfsutil` commands, such as `acfsutil encr` commands, are not allowed in the batch file. If a command in the batch file fails, subsequent commands in the batch file are not run.

The following are examples of commands that can be in a batch file:

```
acfsutil sec realm create my_realm1 -m /mnt1 -e off
acfsutil sec realm create my_realm2 -m /mnt2 -e off
```

Only a security administrator can run this command. When the command is run, the administrator is prompted once for a password.

Examples

The following example shows the use of the `acfsutil sec batch` command.

Example 44 Using the `acfsutil sec batch` command

```
$ /sbin/acfsutil sec batch my_batch_file
```

acfsutil sec disable

Purpose

Disables Oracle ACFS security on a mount point or a realm in a mount point.

Syntax and Description

```
acfsutil sec disable -h
acfsutil sec disable -m mount_point [-S snap_name] [realm]
```

`acfsutil sec disable -h` displays help text and exits.

[Table 52](#) contains the options available with the `acfsutil sec disable` command.

Table 52 Options for the `acfsutil sec disable` command

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.
<code>-S <i>snap_name</i></code>	Disables security for the specified read-write snapshot.
<code><i>realm</i></code>	Specifies the name of the security realm in the Oracle ACFS file system.

The `acfsutil sec disable -m mount_point` command disables security functionality on the Oracle ACFS file system specified by the mount point option. When security is disabled on the file system, security realms do not enforce realm authorization.

The `acfsutil sec disable -m mount_point realm` command disables security for the realm specified in the command.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec disable` command.

Example 45 Using the `acfsutil sec disable` command

```
$ /sbin/acfsutil sec disable -m /acfsmounts/acfs1 my_realm
```

acfsutil sec enable

Purpose

Enables Oracle ACFS security on a mount point or a realm in a mount point.

Syntax and Description

```
acfsutil sec enable -h
acfsutil sec enable -m mount_point [-S snap_name] [realm]
```

`acfsutil sec enable -h` displays help text and exits.

[Table 53](#) contains the options available with the `acfsutil sec enable` command.

Table 53 Options for the `acfsutil sec enable` command

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.
<code>-S <i>snap_name</i></code>	Enables security for the specified read-write snapshot.
<code><i>realm</i></code>	Specifies the name of the security realm.

The `acfsutil sec enable -m mount_point` command enables security functionality on the Oracle ACFS file system specified by the mount point option.

When security is enabled on the file system, security realms that have been enabled enforce realm authorization. You should run this command before enabling any individual security realm.

The `acfsutil sec enable -m mount_point realm` command enables security for the realm specified in the command. The realm enforces authorization if security has been enabled on the file system.

Only a security administrator can run this command.

Examples

These example shows the use of the `acfsutil sec enable` command.

Example 46 Using the `acfsutil sec enable` command

```
$ /sbin/acfsutil sec enable -m /acfsmounts/acfs1
$ /sbin/acfsutil sec enable -m /acfsmounts/acfs1 my_realm
```

acfsutil sec info

Purpose

Displays information about Oracle ACFS security.

Syntax and Description

```
acfsutil sec info -h
acfsutil sec info -m mount_point
    [{-n [realm] | -l [rule] | -s [ruleset] | -c }] [-S snap_name]
```

`acfsutil sec info -h` displays help text and exits.

[Table 54](#) contains the options available with the `acfsutil sec info` command.

Table 54 Options for the `acfsutil sec info` command

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.
<code>-n <i>realm</i></code>	Displays information about the specified security realm. If the realm name is omitted, a list of all realms is displayed.
<code>-l <i>rule</i></code>	Displays information about the specified rule. If the rule name is omitted, a list of all rules is displayed.
<code>-s <i>ruleset</i></code>	Displays information about the specified rule set. If the rule set name is omitted, a list of all rule sets is displayed.
<code>-c</code>	Lists all the command rules.
<code>-S <i>snap_name</i></code>	Displays information about the realms, rules, and rule sets in the specified snapshot.

The `acfsutil sec info` command retrieves information about the list of realms, rules, and rule sets on the specified mount point. By specifying a particular realm, rule, or ruleset, you can retrieve information specific about the specified realm, rule, or ruleset. You can also display information about a specified snapshot.

If the `-m` option is specified without any other options, then the security enabled status and prepared status are displayed for the specified mount point.

To access files in the system security realms, the user should be assigned as a security administrator with the `acfsutil sec admin add` command. Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec info` command.

Example 47 Using the `acfsutil sec info` command

```
$ /sbin/acfsutil sec info -m /acfsmounts/acfs1 -n my_realm
```

acfsutil sec info file

Purpose

Lists the names of the Oracle ACFS security realms that the specified file or directory belongs to.

Syntax and Description

```
acfsutil sec info file -h
acfsutil sec info file -m mount_point path
```

`acfsutil sec info file -h` displays help text and exits.

[Table 55](#) contains the options available with the `acfsutil sec info file` command.

Table 55 Options for the `acfsutil sec info file` command

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.
<code><i>path</i></code>	Specifies the path of the file or directory in the file system.

This command also displays the encryption status of files.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec info file` command.

Example 48 Using the `acfsutil sec info file` command

```
$ /sbin/acfsutil sec info file -m /acfsmounts/acfs1
                               /acfsmounts/acfs1/myfiles
```

acfsutil sec init

Purpose

Initializes Oracle ACFS security.

Syntax and Description

```
acfsutil sec init -h
acfsutil sec init -u admin -g admin_sec_group
```

`acfsutil sec init -h` displays help text and exits.

Table 56 contains the options available with the `acfsutil sec init` command.

Table 56 Options for the `acfsutil sec init` command

Option	Description
<code>-u admin</code>	Specifies the first security administrator user name. The user specified must be an existing operating system (OS) user and a member of the operating system group specified by the <code>-g</code> option. On Windows, the security administrator user name must be specified with a fully qualified user name in the form of <code>domain_name\username</code> .
<code>-g admin_sec_group</code>	Specifies the name of the security group for the administrator. The group specified must be an existing operating system (OS) group. On Windows, the group name must be specified with a fully qualified domain group name in the form of <code>domain_name\groupname</code> . If the <code>domain_name\groupname</code> contains a space, then enclose the string in quotes (" ").

The `acfsutil sec init` command creates the storage necessary for security credentials and identifies an operating system user as the first security administrator. The command also identifies the operating system group that is the designated security group. All users that are security administrators must be members of the designated security group. Security administrators are common for all Oracle ACFS file systems.

If you are setting up an OS user and OS group, refer to your operating system-specific (OS) documentation for information.

The `acfsutil sec init` command is run once to set up Oracle ACFS security for each cluster and can be run from any node in the cluster. Other security commands can also be run from any node in a cluster.

Only the root user or Windows Administrator user can run this command. The user specifies a password for the security administrator. The security administrator password must conform to the following format:

- The maximum number of characters is 20.
- The minimum number of characters is 8.
- The password must contain at least one digit.
- The password must contain at least one letter.

The new security administrator can change the password with the `acfsutil sec admin password` command. For information, refer to "[acfsutil sec admin password](#)".

Security administrators are allowed to browse all directories in an Oracle ACFS file system whether they have the underlying operating system permissions and whether any realm checks allow it. This exception enables a security administrator to check the location of the files when securing them with Oracle ACFS security realms. However, a security administrator cannot view the contents of individual files without the appropriate operating system and security realm permissions.

Examples

The following example shows the use of the `acfsutil sec init` command.

Example 49 Using the acfsutil sec init command

```
$ /sbin/acfsutil sec init -u grid -g asmadmin
```

acfsutil sec load**Purpose**

Loads Oracle ACFS security metadata into a file system identified by a mount point.

Syntax and Description

```
acfsutil sec load -h
acfsutil sec load -m mount_point -p file
```

acfsutil sec load -h displays help text and exits.

Table 57 contains the options available with the acfsutil sec load command.

Table 57 Options for the acfsutil sec load command

Option	Description
-m <i>mount_point</i>	Specifies the directory where the file system is mounted.
-p <i>file</i>	Specifies the name of an existing saved security metadata file.

The acfsutil sec load command loads the security metadata in a saved XML file into the specified Oracle ACFS file system.

To run the acfsutil sec load command, the destination mount point must have a file system that has been prepared for security and does not contain any user-created security objects.

If the file system mounted on destination mount point contains security objects, then you must run acfsutil sec prepare -u to remove all previously created security objects on the file system. After successfully running acfsutil sec prepare -u, you must run acfsutil sec prepare to prepare the file system for security. After successfully running acfsutil sec prepare, you can run acfsutil sec load on the file system. For information about preparing security on or removing security from a file system, refer to “[acfsutil sec prepare](#)”.

The acfsutil sec load command does not load system security realms from the backup file. System security realms are created with the acfsutil sec prepare command; acfsutil sec load does not re-create these realms. For information about the system-created security realms, refer to “[acfsutil sec prepare](#)”.

Only a security administrator can run this command.

Examples

The following example shows the use of the acfsutil sec load command.

Example 50 Using the acfsutil sec load command

```
$ /sbin/acfsutil sec load -m /acfsmounts/acfs1 -p my_metadata_file.xml
```

acfsutil sec prepare**Purpose**

Prepares an Oracle ACFS file system for security features.

Syntax and Description

```
acfsutil sec prepare -h
acfsutil sec prepare [-u] -m mount_point
```

`acfsutil sec prepare -h` displays help text and exits.

[Table 58](#) contains the options available with the `acfsutil sec prepare` command.

Table 58 Options for the `acfsutil sec prepare` command

Option	Description
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-u</code>	<p>Backs out security for the specified mount point. This command removes security from in the file system and reverts the file system to the state before <code>acfsutil sec prepare</code> was run on the file system.</p> <p>This command removes all realm-secured files and directories from the realms and then destroys all Oracle ACFS security rules, rule sets and realms from the file system. However, the <code>.Security</code> directory and its contents, including log files and the security metadata backup files, are not deleted. If you want to remove encryption and security is being used, then this command must be run before encryption is backed out. To back out encryption, refer to "acfsutil encr set".</p>

The `acfsutil sec prepare` command must be run before any of the realm management commands. This command prepares the specified Oracle ACFS file system for security and by default turns security on for the file system.

When running `acfsutil sec prepare -u`, ensure that no other Oracle ACFS security commands are run until `acfsutil sec prepare` has completed.

If auditing is initialized on a cluster, this command also enables an Oracle ACFS security auditing source on the file system. The actions performed when enabling this audit source are the same as those done when the `acfsutil audit enable` command is run directly. For more information, refer to "[acfsutil audit enable](#)".

This command creates the `/mount_point/.Security/`, `/mount_point/.Security/backup`, and `/mount_point/.Security/realm/logs` directories where `mount_point` is the option specified in the command line.

This command creates the following system security realms:

- `SYSTEM_Logs`

This is a system-created realm to protect the Oracle ACFS security log files in the directory `.Security/realm/logs/` directory.
- `SYSTEM_Audit`

This is a system-created realm to protect audit trail files. This realm is created if auditing has been initialized. If auditing has not been initialized, it is created when auditing is enabled for the security source through the `acfsutil audit enable` command. This realm secures the audit trail file so that the audit manager can read and write and the auditor can read the file, and no one else has access. This realm also protects the audit trail file so the audit manager cannot delete (without running the `acfsutil audit purge` command), truncate, overwrite, or `chmod` the file.
- `SYSTEM_SecurityMetadata`

This is a system-created realm to protect the Oracle ACFS metadata XML file in the directory `.Security/backup/` directory.

- `SYSTEM_Antivirus`

This is a system-created realm that allows access for the antivirus software that is running on an Oracle ACFS file system. For every realm protected file or directory, the `SYSTEM_Antivirus` realm is evaluated when authorization checks are performed to determine if the `SYSTEM_Antivirus` realm allows access to the file or directory.

To allow the antivirus process to access realm-protected files or directories, you must add the `LocalSystem` or `SYSTEM` group to the realm with the `acfsutil sec realm add` command, as shown in [Example 52](#). If other antivirus processes are running as `Administrator`, then the user `Administrator` must be added to the `SYSTEM_Antivirus` realm to allow access to realm protected files and directories.

If no Antivirus products have been installed, do not add any users or groups to the `SYSTEM_Antivirus` realm. Because users or groups added to the `SYSTEM_Antivirus` realm have `READ` and `REaddir` access, limit the users or groups added to this realm. You can restrict the time window when the users or groups of this realm can access the realm protected files or directories with time-based rules. You can also have application-based rules if you can identify the process name for the antivirus installation that scans the files.

The `SYSTEM_Antivirus` realm can only perform the following operations on a file or directory: `OPEN`, `READ`, `REaddir`, and setting time attributes. To remove or delete files or directories, you may need to disable security to clean up the infected files.

This realm is set up only for Windows systems.

- `SYSTEM_BackupOperators`

This is a system-created realm that enables you to authorize users that can back up realm-secured files and directories. You can add users, groups, rule sets, and command rules to this realm to provide fine-grain authorization for backing up realm-secured files and directories. A user must be added to this realm to back up realm-secured files and directories.

Use caution when adding groups to this system realm. After you add a group to this system realm, all the users of the added group are able to override the realm protections to access files.

To access files in the system security realms, the user should be assigned as a security administrator with the `acfsutil sec admin add` command.

You can add users, groups, rule sets, and command rules to system-created realms with the `acfsutil sec realm add` command, the same as for user-created realms. However, adding files and directories to system realms is not recommended. You can use the `acfsutil sec realm delete` command to delete objects from the system-created realms.

System-created security realms cannot be removed by a security administrator with the `acfsutil sec admin destroy` command. These realms are only removed when security is backed out of a file system when executing the `acfsutil sec prepare` command with the `-u` option.

The `acfsutil sec prepare -u` command is not allowed if any snapshots exist in the file system.

Only a security administrator can run the `acfsutil sec prepare` command.

Examples

The following example shows the use of the `acfsutil sec prepare` command.

Example 51 Using the `acfsutil sec prepare` command

```
$ /sbin/acfsutil sec prepare -m /acfsmounts/acfs1
```

acfsutil sec realm add

Purpose

Adds objects to an Oracle ACFS security realm.

Syntax and Description

```
acfsutil sec realm add -h
acfsutil sec realm add realm -m mount_point
    {[-u user, ...] [-G os_group, ...]
    [-l commandrule:ruleset, commandrule:ruleset, ...]
    [-e [-a {AES}] [-k {128|192|256}]]
    [-f [-r] path ...]}
```

`acfsutil sec realm add -h` displays help text and exits.

[Table 59](#) contains the options available with the `acfsutil sec realm add` command.

Table 59 Options for the `acfsutil sec realm add` command

Option	Description
<code>realm</code>	Specifies the realm name to add.
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-u user</code>	Specifies user names to add.
<code>-G os_group</code>	Specifies the operating system groups to add.
<code>-l commandrule:ruleset</code>	Specifies the filters to add. The <code>commandrule</code> switch is used to add one or more command rules to the realm with a rule set. <code>ruleset</code> specifies the rule set associated with the command rule for this realm. Only one rule set can be included with each command rule. For a list of command rules, refer to Table 60 . To display a list of the command rules, use <code>acfsutil sec info</code> with the <code>-c</code> option. Refer to " acfsutil sec info ".
<code>-e</code>	Enables encryption on the realm. Turning encryption on for the realm causes all files contained in the realm to be encrypted. These files remain encrypted until they are no longer part of an encrypted realm. Files that are encrypted are not re-encrypted to match the new specified encryption parameters.
<code>-a {AES}</code>	Specifies the encryption algorithm for the realm.
<code>-k { 128 192 256 }</code>	Specifies the encryption key length.
<code>-f [-r] path ...</code>	Adds files specified by <code>path</code> to the realm. <code>-r</code> specifies a recursive operation. File paths must be separated by spaces and must be placed at the end of the command.

Option	Description
	If a specified file is not realm secured, the file is encrypted or decrypted to match the encryption status for the realm.

The `acfsutil sec realm add` command adds objects to the specified realm. The objects to be added include users, groups, command rules, rule sets, and files. If the command encounters an error when adding an object, a message is displayed and the command continues processing the remaining objects.

Multiple entries can be added in a comma-delimited list when adding users, operating system groups, or command rules. Do not use spaces in the comma-delimited list. If spaces are added, then enclose the list in quotes.

If the `-e` option is specified, then encryption must have been initialized for the cluster and set on the file system. For more information, refer to “[acfsutil encr init](#)” and “[acfsutil encr set](#)”.

If the entire mount point, which includes the `.Security` directory, is added to the realm then the security administrator operating system group should be added to the realm to maintain security logging and backing up operations.

The supported command rules are listed in [Table 60](#). These command rules restrict or protect against file system operations on realm-secured files and directories.

Table 60 Command Rules

Rule	Description
ALL	Protects against all file system operations on files and directories.
APPENDFILE	Restricts against additions to the end of a file. Restrictions include writes that start within the current file size, but proceed beyond the end of the file.
CHGRP	Protects from changing the group ownership on a file or directory.
CHMOD	Protects from changing the permissions on a file or directory.
CHOWN	Protects from changing the owner information of a file or directory.
CREATEFILE	Protects from creation of new file in a directory.
DELETEFILE	Protects from deletion of a file from a directory.
EXTEND	Restricts the extension operation of a file size. A file size may still be modifiable with other operations. <code>EXTEND</code> does not protect against a <code>truncate</code> followed by an <code>append</code> operation.
IMMUTABLE	Denies any changes to the files and directories in the realm except changes to extended attributes resulting from commands such as <code>acfsutil tag</code> and <code>acfsutil encr</code> . Includes the following protection for a file or directory: <code>APPENDFILE</code> , <code>CHGRP</code> , <code>CHMOD</code> , <code>CHOWN</code> , <code>DELETEFILE</code> , <code>EXTEND</code> , <code>OVERWRITE</code> , <code>RENAME</code> , <code>RMDIR</code> , <code>TRUNCATE</code> , and <code>WRITE</code> . <code>IMMUTABLE</code> does not deny any changes to the <code>atime</code> attribute. The <code>atime</code> attribute changes when a user accesses the file. Can be set to archive the files and directories in a security realm.
LINKFILE	Restricts the creation of hard links to files.

Rule	Description
MKDIR	Protects from the creation of new directory in a directory.
MMAPREAD	Protects a file from being memory mapped for a read operation using <code>mmap()</code> on Linux or using <code>CreateFileMapping</code> followed by <code>MapViewOfFile()</code> on Windows.
MMAPWRITE	Protects a file from being memory mapped for a write operation. Setting <code>MMAPWRITE</code> also protects a file from mapping for read as the operating system maps a file for both read and write.
OPENFILE	Protects from the opening of a file.
OVERWRITE	Prevents existing content in a file from being overwritten with a write operation whose start and end offsets are within the current file size. If the operations on a file are <code>truncate</code> followed by <code>append</code> , <code>OVERWRITE</code> does not protect the file. To provide additional protection from both <code>append</code> and <code>overwrite</code> operations, use the <code>WRITE</code> command rule.
READDIR	Restricts for a directory listing, except for use by the security administrator group.
READ	Protects from reading the contents of a file. <code>READ</code> also protects against read operations using <code>mmap(2)</code> .
RENAME	Protects against renaming a file or directory.
RMDIR	Protects against removing a directory.
SYMLINK	Restricts the creation of symbolic links in the directories protected by a security realm. When creating symbolic links, it does not matter whether the source file is protected by a security realm.
TRUNCATE	Restricts the truncation of a file.
WRITE	Protects a file against the <code>write</code> system call. <code>WRITE</code> also protects against <code>append</code> and <code>overwrite</code> operations, plus write operations using <code>mmap(2)</code> . A file may still be modifiable with other file operations. To protect the file from other modifications, also use the <code>TRUNCATE</code> and <code>DELETEFILE</code> command rules.

Only a security administrator can run this command.

Examples

[Example 52](#) shows the use of the `acfsutil sec realm add` command. The first `acfsutil sec` command adds a user group to a security realm. The second and third commands add the `LocalSystem` or `SYSTEM` group to the `SYSTEM_Antivirus` realm in a Windows environment.

Example 52 Using the `acfsutil sec realm add` command

```
$ /sbin/acfsutil sec realm add my_security_realm -m /acfsmounts/acfs1
  -G my_os_group

C:\> acfsutil sec realm add SYSTEM_Antivirus /m e: /G "NT AUTHORITY\SYSTEM"

C:\> acfsutil sec realm add SYSTEM_Antivirus /m e: /G "SYSTEM"
```

acfsutil sec realm audit disable

Purpose

Disables auditing of a specific command rule or all command rules for files in an Oracle ACFS security realm.

Syntax and Description

```
acfsutil sec realm audit disable -h
acfsutil sec realm audit disable realm -m mount_point
[-l commandrule,commandrule,...] {-a |-v }
```

`acfsutil sec realm audit disable -h` displays help text and exits.

[Table 61](#) contains the options available with the `acfsutil sec realm audit disable` command.

Table 61 Options for the `acfsutil sec realm audit disable` command

Option	Description
<code>realm</code>	Specifies the security realm name.
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-l commandrule</code>	Specifies the command rules on which to disable auditing. If this option is not specified, then the list of all command rules is the default. For a list of command rules, refer to Table 60 . To display a list of the command rules, use <code>acfsutil sec info</code> with the <code>-c</code> option. Refer to “ acfsutil sec info ”.
<code>-a -v</code>	Specifies to disable audit realm authorizations (<code>-a</code>) or disable audit realm violations (<code>-v</code>). Either <code>-a</code> or <code>-v</code> must be specified.

Multiple entries can be added in a comma-delimited list when listing command rules. Do not use spaces in the comma-delimited list. If spaces are added, then enclose the list in quotes.

Only a security administrator can run this command. This command is authenticated using the Oracle ACFS security administrator password.

Examples

[Example 53](#) shows the use of the `acfsutil sec realm audit disable` command. This command disables auditing on the `OPEN` (all violations) and `WRITE` (all violations) command rules.

Example 53 Using the `acfsutil sec realm audit disable` command

```
$ /sbin/acfsutil sec realm audit disable mySecureRealm
-m /acfsmounts/acfs1 -l OPEN,WRITE -v
```

acfsutil sec realm audit enable

Purpose

Enables auditing of a specific command rule or all command rules for files in an Oracle ACFS security realm.

Syntax and Description

```
acfsutil sec realm audit enable -h
acfsutil sec realm audit enable realm -m mount_point
    [-l commandrule,commandrule,...]
    [-a ] [-v [ -u ] ]
```

`acfsutil sec realm audit enable -h` displays help text and exits.

[Table 62](#) contains the options available with the `acfsutil sec realm audit enable` command.

Table 62 Options for the `acfsutil sec realm audit enable` command

Option	Description
<i>realm</i>	Specifies the security realm name.
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-l commandrule</code>	Specifies the command rules on which to enable auditing. If this option is not specified, then the list of all command rules is the default. For a list of command rules, refer to Table 60 . To display a list of the command rules, use <code>acfsutil sec info</code> with the <code>-c</code> option. Refer to “ acfsutil sec info ”.
<code>-a</code>	Specifies to audit realm authorizations.
<code>-v [-u]</code>	Specifies to audit realm violations. If <code>-u</code> is also specified, only realm violations by users who are members of a realm are audited.

If the `acfsutil sec realm audit enable` command is run multiple times, then the earlier configuration is not negated and the new settings are also applied. An exception to this behavior occurs when the command is run with the `-v` option and the specified command rule has auditing set for realm violations. In this case, the behavior is updated according to whether the `-u` flag was specified. For more information, see [Example 56](#).

Multiple entries can be added in a comma-delimited list when listing command rules. Do not use spaces in the comma-delimited list. If spaces are added, then enclose the list in quotes.

If neither `-a` or `-v` are specified with the `acfsutil sec realm audit enable` command, the default is `-v`. Both `-a` and `-v` can be specified.

Only a security administrator can run this command. This command is authenticated using the Oracle ACFS security administrator password.

Examples

[Example 54](#) shows how to enable auditing of the Oracle ACFS backup operators. Because these users are allowed access to files through the `SYSTEM_Backup` realm and are granted special privileges that give them access to all files on the file system, a security administrator may want to audit their actions. After the command is executed, any time a member of the `SYSTEM_Backup` realm opens a file an audit record is written to the Oracle ACFS Security audit trail on the file system.

Example 54 Auditing Oracle ACFS security backup operators

```
$ /sbin/acfsutil sec realm audit enable SYSTEM_Backup
    -m /acfsmounts/acfs1 -l OPEN -a
```

[Example 55](#) shows how to use the `-u` option to audit realm violations by users who are part of the realm. In this scenario sensitive human resources information is stored in `HumanResources` security realm and the `hr` group is allowed to access this information. However, a ruleset applied to the `ALL` command rule prevents access to this data from 6 PM to 8 AM. With this command, the security administrator could discover if any human resource employees are attempting to access sensitive data outside of the allowed time period. After this command is executed, only access violations by users who are members of the `hr` group are audited.

Example 55 Auditing only security realm users

```
$ /sbin/acfsutil sec realm audit enable HumanResources
-m /acfsmounts/acfs1 -l ALL -v -u
```

[Example 56](#) shows multiple runs of the `acfsutil sec realm audit enable` command. After run 1, the `OPEN` (all violations) and `WRITE` (all violations) command rules are audited. After run 2, the `OPEN` (all violations), `WRITE` (all violations), and `DELETEFILE` (authorizations) command rules are audited. After run 3, the `OPEN` (authorizations and realm user violations), `WRITE` (all violations), `DELETEFILE` (authorizations), and `TRUNCATE` (authorizations and realm user violations) command rules are audited. After run 4, all violations are audited on all command rules. In addition, authorizations are audited for `OPEN`, `DELETEFILE`, and `TRUNCATE`.

Example 56 Running acfsutil sec realm audit enable multiple times

```
$ echo run 1
$ /sbin/acfsutil sec realm audit enable mySecureRealm
-m /acfsmounts/acfs1 -l OPEN,WRITE -v

$ echo run 2
$ /sbin/acfsutil sec realm audit enable mySecureRealm
-m /acfsmounts/acfs1 -l DELETEFILE -a

$ echo run 3
$ /sbin/acfsutil sec realm audit enable mySecureRealm
-m /acfsmounts/acfs1 -l OPEN,TRUNCATE -a -v -u

$ echo run 4
$ /sbin/acfsutil sec realm audit enable mySecureRealm
-m /acfsmounts/acfs1 -v
```

acfsutil sec realm audit info

Purpose

Displays the realm auditing information for a specified Oracle ACFS security realm.

Syntax and Description

```
acfsutil sec realm audit info -h
acfsutil sec realm audit info -m mount_point -n realm
```

`acfsutil sec realm audit info -h` displays help text and exits.

[Table 62](#) contains the options available with the `acfsutil sec realm audit info` command.

Table 63 Options for the `acfsutil sec realm audit info` command

Option	Description
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-n realm</code>	Specifies the security realm name.

The `acfsutil sec realm audit info` command provides information about a specified Oracle ACFS security realm.

Examples

[Example 57](#) shows an example of the `acfsutil sec realm audit info` command.

Example 57 Running `acfsutil sec realm audit info`

```
$ /sbin/acfsutil sec realm audit info -m /acfsmounts/acfs1
-n mySecureRealm
```

```
Command rule auditing information for realm 'mySecureRealm'
on mount point '/acfsmounts/acfs1':
```

```
Realm authorization           : 'READ, WRITE'
Realm violation for all users : 'READ, OPENFILE'
Realm violation for realm users: 'None'
```

acfsutil sec realm clone

Purpose

Clones an Oracle ACFS security realm.

Syntax and Description

```
acfsutil sec realm clone -h
acfsutil sec realm clone realm -s src_mount_point new_realm
[-e] [-f] [-G] [-l] [-u]
acfsutil sec realm clone realm -s src_mount_point
[new_realm] -d destination_mount_point
[-e] [-G] [-l] [-u]
```

`acfsutil sec realm clone -h` displays help text and exits.

[Table 64](#) contains the options available with the `acfsutil sec realm clone` command.

Table 64 Options for the `acfsutil sec realm clone` command

Option	Description
<code>realm</code>	Specifies the realm name to be cloned.
<code>-s src_mount_point</code>	Specifies the directory where the source file system is mounted.
<code>new_realm</code>	Specifies the new realm name.
<code>-d destination_mount_point</code>	Specifies the directory for the destination mount point for the new realm.
<code>-e</code>	Copy encryption attributes to the new realm.
<code>-f</code>	Copy file objects to the new realm.

Option	Description
-G	Copy operating system groups to the new realm.
-l	Copy filters to the new realm.
-u	Copy users to the new realm.

The `acfsutil sec realm clone` makes a copy of the specified realm in the destination mount point. If the source and mount points are different and the new realm name is not specified, then the realm is cloned using the existing realm name in the Oracle ACFS file system specified by destination mount point. If the destination mount point is not specified, then the cloned realm is located in the source mount point and a new unique realm name must be specified.

If the `-l` option is specified and the destination mount point is different than the source mount point, then the rules and rule sets must be cloned first.

If the `-e` option is specified and the destination mount point is different than the source mount point, then encryption must be set on destination mount point. For more information, refer to “[acfsutil encr set](#)”.

The `-f` option can only be used if the destination mount point is the same as the source mount point.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec realm clone` command.

Example 58 Using the `acfsutil sec realm clone` command

```
$ /sbin/acfsutil sec realm clone my_security_realm -s /acfsmounts/acfs1
my_new_security_realm -d /acfsmounts/acfs2 -G
```

acfsutil sec realm create

Purpose

Creates an Oracle ACFS security realm.

Syntax and Description

```
acfsutil sec realm create -h
acfsutil sec realm create realm -m mount_point
-e { on -a {AES} -k {128|192|256} | off }
[-o {enable|disable}] [-d "description"]
```

`acfsutil sec realm create -h` displays help text and exits.

[Table 65](#) contains the options available with the `acfsutil sec realm create` command.

Table 65 Options for the `acfsutil sec realm create` command

Option	Description
<i>realm</i>	Specifies the realm name.
<code>-m mount_point</code>	Specifies the mount point for the file system. A mount point is specified as a path on Linux platforms.

Option	Description
-e {on off}	Specifies encryption on or off for the realm.
-a {AES}	Specifies the encryption algorithm.
-k { 128 192 256 }	Specifies the encryption key length.
-o {enable disable}	Specifies where security is on or off for the realm.
-d "description"	Specifies a realm description.

The `acfsutil sec create realm` creates a new realm in the specified Oracle ACFS file system. The new realm name must be unique in the file system identified by the mount point.

A maximum of 500 Oracle ACFS security realms can be created, including any default system realms created by the `acfsutil sec prepare` command.

The realm is enabled by default unless the `-o disable` option is specified.

If the `-e on` option is specified, then encryption must have been initialized for the cluster and set on the file system. For more information, refer to “[acfsutil encr init](#)” and “[acfsutil encr set](#)”.

If the `-e off` option is specified, you cannot specify the `-a` and `-k` options.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec realm create` command.

Example 59 Using the `acfsutil sec realm create` command

```
$ /sbin/acfsutil sec realm create my_security_realm -m /acfsmounts/acfs1
-e on -a AES -k 192 -o enable
```

acfsutil sec realm delete

Purpose

Deletes objects from an Oracle ACFS security realm.

Syntax and Description

```
acfsutil sec realm delete -h
acfsutil sec realm delete realm -m mount_point
    {[-u user, ...] [-G os_group, ...]
    [-l :ruleset,commandrule:ruleset, ...]
    [-f [-r] path, ...] } [-e ]
```

`acfsutil sec realm delete -h` displays help text and exits.

[Table 66](#) contains the options available with the `acfsutil sec realm delete` command.

Table 66 Options for the `acfsutil sec realm delete` command

Option	Description
<i>realm</i>	Specifies the realm name.

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.
<code>-u <i>user</i></code>	Specifies user names to delete.
<code>-G <i>os_group</i></code>	Specifies the operating system groups to delete.
<code>-l</code> <code><i>commandrule:ruleset</i></code>	Specifies the filters to delete from the realm. To display a list of the command rules, use <code>acfsutil sec info</code> with the <code>-c</code> option. <i>ruleset</i> specifies the rule set associated with the command rule for this realm.
<code>-f [-r] <i>path</i> ...</code>	Deletes files specified by <i>path</i> from the realm. <code>-r</code> specifies a recursive operation. File paths must be separated by spaces. If this is the last realm securing the file, the file is encrypted or decrypted to match the file system level encryption state.
<code>-e</code>	Disables encryption on the realm. When disabling encryption, this option decrypts any files in the realm that do not belong to any other encrypted realms. If a file is part of another realm which is encrypted or if encryption is turned on for the file system, then the file remains encrypted.

The `acfsutil sec realm delete` command removes objects from the specified realm. The objects to be deleted include users, groups, rule sets, and files. If the command encounters an error when deleting an object, a message is displayed and the command continues processing the remaining objects.

Multiple entries can be added in a comma-delimited list when adding users, operating system groups, or command rules. Do not use spaces in the comma-delimited list. If spaces are added, then enclose the list in quotes.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec realm delete` command.

Example 60 Using the `acfsutil sec realm delete` command

```
$ /sbin/acfsutil sec realm delete my_security_realm -m /acfsmounts/acfs1
-f -r /acfsmounts/acfs1/myoldfiles/*.log
```

acfsutil sec realm destroy

Purpose

Destroys an Oracle ACFS security realm.

Syntax and Description

```
acfsutil sec realm destroy -h
acfsutil sec realm destroy realm -m mount_point
```

`acfsutil sec realm destroy -h` displays help text and exits.

[Table 67](#) contains the options available with the `acfsutil sec realm destroy` command.

Table 67 Options for the `acfsutil sec realm destroy` command

Option	Description
<code>realm</code>	Specifies the realm name.
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.

The `acfsutil sec destroy realm` removes a security realm from the specified Oracle ACFS file system. Destroying the realm does not destroy the objects in the realm; this command simply removes the security associated with the realm from the objects.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec realm destroy` command.

Example 61 Using the `acfsutil sec realm destroy` command

```
$ /sbin/acfsutil sec realm destroy my_security_realm -m /acfsmounts/acfs1
```

acfsutil sec rule clone

Purpose

Clones a security rule.

Syntax and Description

```
acfsutil sec rule clone -h
acfsutil sec rule clone rule -s src_mount_point new_rule
acfsutil sec rule clone rule -s src_mount_point
    [new_rule] -d mount_point
```

`acfsutil sec rule clone -h` displays help text and exits.

[Table 68](#) contains the options available with the `acfsutil sec rule clone` command.

Table 68 Options for the `acfsutil sec rule clone` command

Option	Description
<code>rule</code>	Specifies the existing name of the rule. If the name contains a space, enclose in quotes (" ").
<code>-s src_mount_point</code>	Specifies the directory where the source file system is mounted.
<code>-d mount_point</code>	Specifies the directory for the destination mount point of the file system.
<code>new_rule</code>	Specifies the new name of the rule. If the name contains a space, enclose in quotes (" ").

If the source and mount points are different and the new rule name is not specified, then the rule is cloned using the existing rule name in the Oracle ACFS file system specified by destination mount point. If the destination mount point is not specified, then the cloned rule is located in the source mount point and a new unique rule name must be specified.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec rule clone` command.

Example 62 Using the `acfsutil sec rule clone` command

```
$ /sbin/acfsutil sec rule clone my_security_rule -s /acfsmounts/acfs1
   my_new_security_rule -d /acfsmounts/acfs2
```

acfsutil sec rule create

Purpose

Creates a security rule.

Syntax and Description

```
acfsutil sec rule create -h
acfsutil sec rule create rule -m mount_point
    -t rule_type rule_value
    [-o {ALLOW|DENY}]
```

`acfsutil sec rule create -h` displays help text and exits.

[Table 69](#) contains the options available with the `acfsutil sec rule create` command.

Table 69 Options for the `acfsutil sec rule create` command

Option	Description
<code>rule</code>	Specifies the name of the rule. If the name contains a space, enclose in quotes (" ").
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-t rule_type rule_value</code>	Specifies a rule type and a rule value. The rule type can be <code>application</code> , <code>hostname</code> , <code>time</code> , or <code>username</code> . The rule value depends on the type of rule. The valid rule types and values are described in this section.
<code>-o option</code>	Specifies options preceded by <code>-o</code> . The option specified can be <code>ALLOW</code> or <code>DENY</code> . The default value is <code>DENY</code> .

The `acfsutil sec rule create` command creates a new rule in the Oracle ACFS file system specified by the mount point. The new rule can be added to a rule set and that rule set can be added to a security realm.

A maximum of 500 Oracle ACFS security rules can be created.

The rule types and associated rule values are:

- `application`
This rule type specifies the name of an application which is allowed or denied access to the objects protected by a realm.
- `hostname`
This rule type specifies the name of a computer from which a user accesses the objects protected by a realm. Access from a node can be allowed or denied using this rule. The `hostname` should be one of the cluster node names and not any

other external nodes which could have mounted the Oracle ACFS file system as a network File System (NFS) mount.

- `time`

This rule type specifies the time interval in the form *start_time,end_time*. This time interval specifies access to a realm. Access can be allowed or denied to objects protected by a realm only during certain times of the day by setting this rule in a realm. The time is based on the local time of the host.

- `username`

This rule type specifies the name of a user to be added or deleted from a realm. You can use this option to deny access for any user that belongs to a security group that is part of a realm.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec rule create` command.

Example 63 Using the `acfsutil sec rule create` command

```
$ /sbin/acfsutil sec rule create my_security_rule -m /acfsmounts/acfs1
-t username security_user_one -o ALLOW
```

acfsutil sec rule destroy

Purpose

Removes a security rule.

Syntax and Description

```
acfsutil sec rule destroy -h
acfsutil sec rule destroy rule -m mount_point
```

`acfsutil sec rule destroy -h` displays help text and exits.

[Table 70](#) contains the options available with the `acfsutil sec rule destroy` command.

Table 70 Options for the `acfsutil sec rule destroy` command

Option	Description
<code>rule</code>	Specifies the name of the rule. If the name contains a space, enclose in quotes (" ").
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.

The `acfsutil sec rule destroy` command removes a rule from the rule sets in the Oracle ACFS file system specified by the mount point. A rule set is not destroyed if all the rules are destroyed. The empty rule set must be explicitly destroyed.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec rule destroy` command.

Example 64 Using the `acfsutil sec rule destroy` command

```
$ /sbin/acfsutil sec rule destroy my_security_rule -m /acfsmounts/acfs1
```

acfsutil sec rule edit**Purpose**

Updates a security rule.

Syntax and Description

```
acfsutil sec rule edit -h
acfsutil sec rule edit rule -m mount_point
    { [-t rule_type rule_value ] [-o {ALLOW|DENY}] }
```

`acfsutil sec rule edit -h` displays help text and exits.

[Table 71](#) contains the options available with the `acfsutil sec rule edit` command.

Table 71 Options for the `acfsutil sec rule edit` command

Option	Description
<code>rule</code>	Specifies the name of the rule. If the name contains a space, enclose in quotes (" ").
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-t rule_type</code> <code>rule_value</code>	Specifies a rule type and a rule value. The rule type can be application, hostname, time, or username. Rule value depends on the type of rule. For information on the rule type and rule value, refer to “ acfsutil sec rule create ”.
<code>-o option</code>	Specifies options preceded by <code>-o</code> . The option specified can be ALLOW or DENY.

The `acfsutil sec rule edit` updates a rule. The value that is associated with a rule can be updated, but not the rule type.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec rule edit` command to update `my_security_rule`. The existing rule is of type `username` and that value cannot be changed.

Example 65 Using the `acfsutil sec rule edit` command

```
$ /sbin/acfsutil sec rule edit my_security_rule -m /acfsmounts/acfs1
    -t username security_user_three -o ALLOW
```

acfsutil sec ruleset clone**Purpose**

Clones a security rule set.

Syntax and Description

```
acfsutil sec ruleset clone -h
acfsutil sec ruleset clone ruleset -s mount_point new_ruleset
```

```
acfsutil sec ruleset clone ruleset -s mount_point
    [new_ruleset] -d mount_point
```

`acfsutil sec ruleset clone -h` displays help text and exits.

[Table 72](#) contains the options available with the `acfsutil sec ruleset clone` command.

Table 72 Options for the `acfsutil sec ruleset clone` command

Option	Description
<i>rule_set</i>	Specifies the existing name of the rule set. If the name contains a space, enclose in quotes (" ").
<code>-s <i>mount_point</i></code>	Specifies the directory where the source file system is mounted.
<code>-d <i>mount_point</i></code>	Specifies the directory for the destination mount point of the file system.
<i>new_rule_set</i>	Specifies the new name of the rule set. If the name contains a space, enclose in quotes (" ").

If the source mount point is different from destination mount point, the rules in the rule set must be cloned first.

If the source and mount points are different and the new rule set name is not specified, then the rule set is cloned using the existing rule set name in the Oracle ACFS file system specified by destination mount point. If the destination mount point is not specified, then the cloned rule set is located in the source mount point and a new unique rule set name must be specified.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec ruleset clone` command.

Example 66 Using the `acfsutil sec ruleset clone` command

```
$ /sbin/acfsutil sec ruleset clone
    my_security_ruleset -s /acfsmounts/acfs1
    my_new_security_ruleset -d /acfsmounts/acfs2
```

acfsutil sec ruleset create

Purpose

Creates a security rule set.

Syntax and Description

```
acfsutil sec ruleset create -h
acfsutil sec ruleset create rule_set -m mount_point
    [-o {ALL_TRUE|ANY_TRUE}]
```

`acfsutil sec ruleset create -h` displays help text and exits.

[Table 73](#) contains the options available with the `acfsutil sec ruleset create` command.

Table 73 Options for the `acfsutil sec ruleset create` command

Option	Description
<code>rule_set</code>	Specifies the name of the rule set. If the name contains a space, enclose in quotes (" ").
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-o option</code>	Specifies options preceded by <code>-o</code> . The option specified can be <code>ALL_TRUE</code> or <code>ANY_TRUE</code> . The default value is <code>ALL_TRUE</code> .

The `acfsutil sec ruleset create` command creates a new rule set in the specified mount point.

A maximum of 500 Oracle ACFS security rule sets can be created.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec ruleset create` command.

Example 67 Using the `acfsutil sec ruleset create` command

```
$ /sbin/acfsutil sec ruleset create
   my_security_ruleset -m /acfsmounts/acfs1 -o ANY_TRUE
```

acfsutil sec ruleset destroy

Purpose

Removes a security rule set.

Syntax and Description

```
acfsutil sec ruleset destroy -h
acfsutil sec ruleset destroy rule_set -m mount_point
```

`acfsutil sec ruleset destroy -h` displays help text and exits.

[Table 74](#) contains the options available with the `acfsutil sec ruleset destroy` command.

Table 74 Options for the `acfsutil sec ruleset destroy` command

Option	Description
<code>rule_set</code>	Specifies the name of the rule set. If the name contains a space, enclose in quotes (" ").
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.

The `acfsutil sec ruleset destroy` command removes a rule set from the Oracle ACFS file system specified by the mount point. Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec ruleset destroy` command.

Example 68 Using the acfsutil sec ruleset destroy command

```
$ /sbin/acfsutil sec ruleset destroy
   my_security_ruleset -m /acfsmounts/acfs1
```

acfsutil sec ruleset edit**Purpose**

Updates a security rule set.

Syntax and Description

```
acfsutil sec ruleset edit -h
acfsutil sec ruleset edit rule_set -m mount_point
    { [-a rule,...] [-d rule,...] [-o {ALL_TRUE|ANY_TRUE}]}
```

acfsutil sec ruleset edit -h displays help text and exits.

Table 75 contains the options available with the acfsutil sec ruleset edit command.

Table 75 Options for the acfsutil sec ruleset edit command

Option	Description
<i>rule_set</i>	Specifies the name of the rule set. If the name contains a space, enclose in quotes (" ").
<i>-m mount_point</i>	Specifies the directory where the file system is mounted.
<i>-a rule</i>	Specifies the rule to add.
<i>-d rule</i>	Specifies the rule to remove.
<i>-o option</i>	Specifies options preceded by -o. The option specified can be ALL_TRUE or ANY_TRUE.

The acfsutil sec ruleset edit command updates a rule set in the Oracle ACFS file system specified by the mount point.

Only a security administrator can run this command.

Examples

The following example shows the use of the acfsutil sec ruleset edit command.

Example 69 Using the acfsutil sec ruleset edit command

```
$ /sbin/acfsutil sec ruleset edit
   my_security_ruleset -m /acfsmounts/acfs1
   -a my_new_rule -o ANY_TRUE
```

acfsutil sec save**Purpose**

Saves Oracle ACFS file system security metadata.

Syntax and Description

```
acfsutil sec save -h
acfsutil sec save -m mount_point -p file
```

`acfsutil sec save -h` displays help text and exits.

[Table 76](#) contains the options available with the `acfsutil sec save` command.

Table 76 Options for the `acfsutil sec save` command

Option	Description
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-p file</code>	Specifies a file name to store the security metadata. The file is saved in the <code>/mount_point/.Security/backup/</code> directory.

The `acfsutil sec save` command saves the security metadata for an Oracle ACFS file system to an XML file. By default, the file is saved in the `/mount_point/.Security/backup` directory.

This file can be backed up as a regular file by a backup application. System realms protect this file and allow only members of these realms to access this file and prevent all other users including the root user and system administrator from access. For information about the system-created security realms, refer to “[acfsutil sec prepare](#)”.

Only a security administrator can run this command.

Examples

The following example shows the use of the `acfsutil sec save` command.

Example 70 Using the `acfsutil sec save` command

```
$ /sbin/acfsutil sec save -m /acfsmounts/acfs1 -p my_metadata_file.xml
```

Oracle ACFS Command-Line Tools for Encryption

[Table 77](#) contains a summary of the commands for Oracle ACFS encryption. For an overview of Oracle ACFS encryption, refer to “[Oracle ACFS Encryption](#)”.

You can run `acfsutil help` on all platforms to display help text. You can run `acfsutil version` on all platforms to display the Oracle ACFS version.

When the options are entered with commands on a Windows platform, use `/` instead of `-` with the option. For example, you can display help for `acfsutil` on a Linux platform with `acfsutil -h`. On a Windows platform, use `acfsutil /h`.

A mount point on a Windows operating system can be a drive letter or a directory including the drive letter. When using a drive letter in a command, include the backslash (`\`) with the drive letter, such as in `M:\`, to avoid the possibility of triggering a Windows path substitution to the last accessed path on the specified drive.

Table 77 Summary of commands for Oracle ACFS encryption

Command	Description
acfsutil encr info	Displays encryption-related information about Oracle ACFS file systems.
acfsutil encr init	Creates storage for encryption keys.

Command	Description
<code>acfsutil encr off</code>	Disables encryption for an Oracle ACFS file system.
<code>acfsutil encr on</code>	Encrypts an Oracle ACFS file system.
<code>acfsutil encr rekey</code>	Generates a new key and re-encrypts an Oracle ACFS file system.
<code>acfsutil encr set</code>	Sets or changes encryption parameters for an Oracle ACFS file system.
<code>acfsutil keystore migrate</code>	Migrates the encryption keystore.

acfsutil encr info

Purpose

Displays encryption-related information about Oracle ACFS file systems, directories, or files.

Syntax and Description

```
acfsutil encr info -h
acfsutil encr info -m mount_point [[-r] path [path ...]]
```

`acfsutil encr info -h` displays help text and exits.

[Table 78](#) contains the options available with the `acfsutil encr info` command.

Table 78 Options for the `acfsutil encr info` command

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.
<code>-r</code>	Specifies recursive action under an existing directory folder identified by <i>path</i> .
<i>path</i>	Specifies the absolute or relative path of a directory. Multiple path values are allowed.

If `-m` is specified without a *path*, the encryption status, algorithm, and key length are displayed for the file system level.

If `-r` is specified with a *path*, the encryption status, algorithm, and key length are displayed for all objects under the directory specified by *path*.

The `acfsutil encr info` command displays encryption status and parameters for files in a snapshot if the files are specified with the *path* option.

This command fails when it is run on realm-secured objects.

Any user can run this command to display encryption information about a file system, directory, or file.

If the `acfsutil encr info` command is run as a system administrator, then the output displays the types of keystore used. The types are single-sign-on wallet in the OCR (SSO), password-protected wallet in the OCR (PKS), and Oracle Key Vault as the key store (OKV).

Examples

The following are examples of the use of `acfsutil encr info`.

Example 71 Using the `acfsutil encr info` command

```
# /sbin/acfsutil encr info -m /acfsmounts/acfs1

# /sbin/acfsutil encr info -m /acfsmounts/acfs1
-r /acfsmounts/acfs1/myfiles
```

acfsutil encr init**Purpose**

Creates storage for encryption keys.

Syntax and Description

```
acfsutil encr init -h
acfsutil encr init [-p ]
```

`acfsutil encr init -h` displays help text and exits.

[Table 79](#) contains the options available with the `acfsutil encr init` command.

Table 79 Options for the `acfsutil encr init` command

Option	Description
-p	Creates PKCS (password-protected) storage for keys.

The `acfsutil encr init` command must be run before any other encryption `acfsutil` commands can be run. This command must be run once for each cluster on which Oracle ACFS encryption is run.

If you plan to use Oracle Key Vault as the key store, then you still must run `acfsutil encr init` first.

See Also:

Oracle Key Vault Administrator's Guide for information about Oracle Key Vault

If the `-p` option is specified, you must provide a password when prompted. The password must conform to the format that is described in "[acfsutil sec init](#)".

If the `-p` option is not specified, a single sign-on (SSO) wallet is created.

Only a user with root or system administrator privileges can run this command.

Examples

The following is an example of the use of `acfsutil encr init`.

Example 72 Using the `acfsutil encr init` command

```
# /sbin/acfsutil encr init
```

acfsutil encr off**Purpose**

Disables encryption for an Oracle ACFS file system, directories, or individual files.

Syntax and Description

```
acfsutil encr off -h
acfsutil encr off -m mount_point [[-r] path [path ...]]
```

`acfsutil encr off -h` displays help text and exits.

[Table 81](#) contains the options available with the `acfsutil encr off` command.

Table 80 Options for the `acfsutil encr off` command

Option	Description
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.
<code>-r</code>	Specifies to disable encryption recursively under an existing directory identified by <i>path</i> .
<i>path</i>	Specifies the absolute or relative path of a directory. Multiple path values are allowed.

This command cannot be run on security realm-protected files.

Only an administrator can run this command on an Oracle ACFS file system (`-m` option without a *path* specified). When the `-m` option is specified without a *path*, all the files under the mount point are decrypted.

The *path* option can specify a path to a file or directory in a read-write snapshot. If the `-r` option is specified with the command on the root directory, the command does not transverse the snapshots under the `.ACFS` directory. If a decryption operation is specified at the file system level, then the operation does not process files and directories of snapshots in the `.ACFS/snaps/` directory.

Only a user with root or system administrator privileges can run this command to disable encryption on a file system. The file owner can also run this command to disable encryption on a directory or file.

Examples

The following are examples of the use of `acfsutil encr off`.

Example 73 Using the `acfsutil encr off` command

```
# /sbin/acfsutil encr off -m /acfsmounts/acfs1
# /sbin/acfsutil encr off -m /acfsmounts/acfs1
                        -r /acfsmounts/acfs1/myfiles
```

acfsutil encr on**Purpose**

Encrypts an Oracle ACFS file system, directories, or individual files.

Syntax and Description

```
acfsutil encr on -h
acfsutil encr on -m mount_point
                    [-a {AES} -k {128|192|256}] [[-r] path [path...]]
```

`acfsutil encr on -h` displays help text and exits.

[Table 81](#) contains the options available with the `acfsutil encr on` command.

Table 81 Options for the `acfsutil encr on` command

Option	Description
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-a algorithm</code>	Specifies the encryption algorithm type for a directory or file. Advanced Encryption Standard (AES) is the only encryption algorithm supported for this release.
<code>-k key_length</code>	Specifies the encryption key length for a directory or file.
<code>-r</code>	Specifies encryption recursively under existing directory folder identified by <i>path</i> .
<i>path</i>	Specifies the absolute or relative path of a directory. Multiple path values are allowed.

This command cannot be run on realm-protected files.

The default values for the `-a` and `-k` are determined by the volume parameters specified when `acfsutil encr set` was run. To set the key length at the volume level, use the `acfsutil encr set` command.

Only an administrator can run this command on an Oracle ACFS file system (`-m` option without a *path* specified). When the `-m` option is specified without a *path*, all the files under the mount point are encrypted.

The *path* option can specify a path to a file or directory in a read-write snapshot. If the `-r` option is specified with the command on the root directory, the command does not transverse the snapshots under the `.ACFS` directory. If an encryption operation is specified at the file system level, then the operation does not process files and directories of snapshots in the `.ACFS/snaps/` directory.

When you run `acfsutil encr on` with the `-r` option, the command encrypts the specified directory recursively, but does not enable encryption on the file system level.

Only a user with root or system administrator privileges can run this command to enable encryption on a file system. The file owner can also run this command to enable encryption on a directory or file.

Examples

The following are examples of the use of `acfsutil encr on`.

Example 74 Using the `acfsutil encr on` command

```
# /sbin/acfsutil encr on -m /acfsmounts/acfs1
# /sbin/acfsutil encr on -m /acfsmounts/acfs1
-a AES -k 128 -r /acfsmounts/acfs1/myfiles
```

acfsutil encr rekey

Purpose

Generates a new key and re-encrypts volume or file.

Syntax and Description

```
acfsutil encr rekey -h
acfsutil encr rekey -m mount_point
{-f [-r] path [path...] |-v } [-a {AES} -k {128|192 |256}]
```

`acfsutil encr rekey -h` displays help text and exits.

Table 82 contains the options available with the `acfsutil encr rekey` command.

Table 82 Options for the `acfsutil encr rekey` command

Option	Description
<code>-m mount_point</code>	Specifies the directory where the file system is mounted.
<code>-f [-r] path ...</code>	Generates a new file encryption key for the specified path and then encrypts the data with the new key. If <code>-r</code> is specified, the rekey operation is performed recursively under <code>path</code> . <code>path</code> specifies the absolute or relative path of a directory. Multiple path values are allowed.
<code>-v</code>	Generates a new volume encryption key (VEK) for the specified mount point and then encrypts all the file encryption keys in file system with the new key. Prompts for the wallet password because the wallet must be accessed to store the new VEK. The generated key is stored in the key store that was previously configured with the <code>acfsutil encr init</code> command.
<code>-a algorithm</code>	Specifies the algorithm. Advanced Encryption Standard (AES) is the only encryption supported for this release.
<code>-k key_length</code>	Specifies the key length for the directory or file specified by <code>path</code> .

This command cannot be run on security realm-protected files.

The default values for the `-a` and `-k` are determined by the volume parameters specified when `acfsutil encr set` was run.

The `path` option can specify a path to a file or directory in a read-write snapshot. If the `-r` option is specified with the command on the root directory, the command does not transverse the snapshots under the `.ACFS` directory. If a rekey operation is specified at the file system level, then the operation does not process files and directories of snapshots in the `.ACFS/snaps/` directory.

If Oracle Key Vault is the key store for the file system, then the Oracle Key Vault home environmental variable (`OKV_HOME`) must be set when using the `-v` option to generate a new volume key. If the client was configured to use a password with Oracle Key Vault, then the same password must be entered when prompted.

See Also:

Oracle Key Vault Administrator's Guide for information about Oracle Key Vault

Only a user with root or system administrator privileges can run this command with the `-v` option. The file owner can also run this command with the `-f` option to rekey encryption on the directory or file.

Examples

The following are examples of the use of `acfsutil encr rekey`.

Example 75 Using the `acfsutil encr rekey` command

```
# /sbin/acfsutil encr rekey -m /acfsmounts/acfs1 -v
```



```
# /sbin/acfsutil encr rekey -m /acfsmounts/acfs1 -f
-r /acfsmounts/acfs1/myfiles
```

acfsutil encr set

Purpose

Sets or changes encryption parameters for an Oracle ACFS file system.

Syntax and Description

```
acfsutil encr set -h
acfsutil encr set [ [-a {AES} -k {128|192|256}] [-e] | -u ] -m mount_point
```

`acfsutil encr set -h` displays help text and exits.

[Table 83](#) contains the options available with the `acfsutil encr set` command.

Table 83 Options for the `acfsutil encr set` command

Option	Description
<code>-a <i>algorithm</i></code>	Specifies the algorithm. Advanced Encryption Standard (AES) is the default value and the only encryption supported for this release. The algorithm must be specified if <code>-k</code> is specified.
<code>-k {128 192 256}</code>	Specifies the key length. The key length is set at the volume level. The default is 192. Must be specified if <code>-a</code> is specified.
<code>-e</code>	Specifies to use Oracle Key Vault as the key store.
<code>-u</code>	Backs out encryption. Decrypts all encrypted files in the file system and reverts the file system to the state before <code>acfsutil encr set</code> was run on the file system. If security is being used, then this command can only be run after security has been backed out. To remove security, refer to “acfsutil sec prepare” .
<code>-m <i>mount_point</i></code>	Specifies the directory where the file system is mounted.

Before running the `acfsutil encr set` command, you must first run the `acfsutil encr init` command.

The `acfsutil encr set` command configures encryption parameters for a file system, transparently generates a volume encryption key, and stores that the generated key in the key store that was previously configured with the `acfsutil encr init` command.

If auditing is initialized on a cluster, this command also enables an Oracle ACFS encryption auditing source on the file system. The actions performed when enabling this audit source are the same as those done when the `acfsutil audit enable` command is run directly. For more information, refer to [“acfsutil audit enable”](#).

In addition `acfsutil encr set` creates the `mount_point/.Security/encryption/logs/` directory that contains the log file (`encr-hostname_fsid.log`) that collects auditing and diagnostic data.

Password requirements when storing the key are dependent on how the encryption key storage was configured. If `-p` was specified with `acfsutil encr init`, then a password is required to run this command.

Before using the `-e` option to specify Oracle Key Vault as the key store, Oracle Key Vault must be configured first. If you want to choose Oracle Key Vault as the key store

for the file system, then the Oracle Key Vault home environmental variable (OKV_HOME) must be set when running the command with the `-e` option. If the client was configured to use a password with Oracle Key Vault, then the same password must be entered when prompted.

See Also:

Oracle Key Vault Administrator's Guide for information about configuring Oracle Key Vault

The `acfsutil encr set -u` command is not allowed if any snapshots exist in the file system.

Only a user with root or system administrator privileges can run the `acfsutil encr set` command.

Examples

The following example shows the use of `acfsutil encr set` command.

Example 76 Using the `acfsutil encr set` command

```
# /sbin/acfsutil encr set -a AES -k 256 -m /acfsmounts/acfs1
```

acfsutil keystore migrate

Purpose

Migrates the encryption keystore.

Syntax and Description

```
acfsutil keystore migrate -h
acfsutil keystore migrate [-p ]
```

`acfsutil keystore migrate -h` displays help text and exits.

[Table 79](#) contains the options available with the `acfsutil keystore migrate` command.

Table 84 Options for the `acfsutil keystore migrate` command

Option	Description
<code>-p</code>	Converts the encryption keystore from a SSO wallet to a PKCS wallet.

If the `-p` option is specified, `acfsutil keystore migrate` converts the SSO wallet to a PKCS wallet. If the `-p` option is not specified, `acfsutil keystore migrate` converts the PKCS wallet to a SSO wallet.

Only a user with root or system administrator privileges can run this command.

Examples

The following is an example of the use of `acfsutil keystore migrate`.

Example 77 Using the `acfsutil keystore migrate` command

```
# /sbin/acfsutil keystore migrate
```

Oracle ACFS Command-Line Utilities

[page 16-107](#) contains a summary of various Oracle ACFS command-line utilities. For an overview of Oracle ACFS snapshots, refer to [“About Oracle ACFS Snapshots”](#). For an overview of Oracle ACFS plugins, refer to [“Oracle ACFS Plugins”](#).

You can use `acfsutil help` on all platforms to display help text. You can run `acfsutil version` on all platforms to display the Oracle ACFS version.

When the options are entered with commands on a Windows platform, use `/` instead of `-` with the option. For example, you can display help for `acfsutil` on a Linux platform with `acfsutil -h`. On a Windows platform, use `acfsutil /h`.

A mount point on a Windows operating system can be a drive letter or a directory including the drive letter. When using a drive letter in a command, include the backslash (`\`) with the drive letter, such as in `M:\`, to avoid the possibility of triggering a Windows path substitution to the last accessed path on the specified drive.

Command	Description
acfsdbg	Debugs an Oracle ACFS file system.
acfsutil info file	Displays information for a file in an Oracle ACFS file system.
acfsutil info fs	Displays detailed Oracle ACFS file system information.
acfsutil info id	Displays Oracle ACFS file system information for a specified file identifier and mount point.
acfsutil plugin disable	Disables the Oracle ACFS plug-in infrastructure.
acfsutil plugin enable	Enables the Oracle ACFS plug-in infrastructure.
acfsutil plugin info	Displays information about the Oracle ACFS plug-in infrastructure.
acfsutil registry	Adds, deletes, or displays entries in the Oracle ACFS mount registry.
acfsutil rmfs	Removes an Oracle ACFS file system.
acfsutil size	Resizes an Oracle ACFS file system.
acfsutil snap convert	Converts the type of an existing snapshot.
acfsutil snap create	Creates a snapshot of an Oracle ACFS file system or an existing snapshot.
acfsutil snap delete	Deletes a snapshot of an Oracle ACFS file system.
acfsutil snap info	Displays information about Oracle ACFS file system snapshots.
acfsutil tune	Modifies or displays Oracle ACFS tunable parameters.
advmutil canonical	Displays the canonical name of an Oracle ADVM volume.
advmutil tune	Modifies or displays Oracle ADVM parameters.
advmutil volinfo	Displays information about Oracle ADVM volumes.

acfsdbg

Purpose

Debugs an Oracle ACFS file system.

Syntax and Description

```
acfsdbg -h
acfsdbg [-r] [-l] volume_device
```

[Table 86](#) contains the options available with the `acfsdbg` command.

Table 86 Options for the `acfsdbg` command

Option	Description
-h	Prints out the usage message which displays the various options that are available when invoking the <code>acfsdbg</code> command, then exits.
-r	Operates in read-only mode. No data is modified on the file system and all write commands are disabled. If the device is mounted anywhere, <code>acfsdbg</code> may not display the latest data because some data is cached by the file system mounts.
-l	Processes kernel log files. The default is to not process the log files.
<i>volume_device</i>	Specifies the device name of the volume.

`acfsdbg` is an extension to `fsck` and `acfschkdsk`, and is an interactive program that views and modifies on disk structures of the file system. This command is intended for experienced development and support engineers to examine on disk structures to diagnose problems. Use with caution.

When `acfsdbg` is started, it displays a command prompt. At the command prompt, you can enter the subcommands listed in [Table 87](#).

You can also use `acfsdbg` for scripts by echoing `acfsdbg` subcommands with a shell pipe to the `acfsdbg` binary.

By default the file system is not modified when running the tool. If the `-l` option is used, the file system metadata in the transaction logs is applied before the interactive disk block dump session. The volume device must specify a volume with a dismounted Oracle ACFS file system. If the volume device has a mounted Oracle ACFS file system, `acfsdbg` displays an error message and exits.

You must be the administrator or a member of the Oracle ASM administrator group to run `acfsdbg`.

Subcommands

[Table 87](#) lists the subcommands of `acfsdbg`.

Table 87 Subcommands for `acfsdbg`

Option	Description	Syntax
calculate	Calculates simple arithmetic expressions Valid operators: + - * / % & ^ ~ <<>> White space starts a new expression	calculate [-v] expr [...] -v Verbose mode

Option	Description	Syntax
	0-1 represents a negative 1	<i>expr</i> Simple 2+2 expression
cksum	Generates and replaces checksum in header Header offset can be an expression as used by the <code>calculate</code> subcommand White space starts a new header offset Command is disabled in read-only mode	<code>cksum [-C -CE] <i>header_offset</i> [...]</code> -C Regenerate for normal structure checksum -CE Re-generate for Extent structure checksum <i>header_offset</i> Offset of the on disk structure header. The value can be an expression as used by the <code>calculate</code> subcommand
close	Closes the open handle to the device	<code>close</code>
echo	Echoes text on command line to stdout	<code>echo</code>
fenum	Displays the specified File Entry Table (FETA) entry	<code>fenum [-f -e -d] <i>FETA_entry_number</i></code> -f Displays all on disk structures related to this structure -e Displays all on disk extent information related to this structure -d Casts the structure as a directory and displays its contents <i>FETA_entry_number</i> The File Entry Table number used to identify a file on the file system
help	Displays help message	<code>help</code>
offset	Displays structure at disk offset	<code>offset [-c <i>cast</i>] [-f -d] <i>disk_offset</i></code> -f Displays all on disk structures related to this structure -d Casts the structure as a directory and displays its contents <i>disk_offset</i> Disk offset to display. The value can be an expression as used by the <code>calculate</code> subcommand
open	Opens a handle to a device. The default is the volume device name entered on the command line	<code>open [<i>volume_device</i>]</code>
primary	Sets the context of commands to the primary file system	<code>primary</code>
prompt	Sets the prompt to the specified string	<code>prompt "<i>prompt_string</i>"</code>
quit	Exits the <code>acfsdbg</code> debugger command	<code>quit</code>
read	Reads value from offset The default size to read in is 8 bytes The default count to read is 1	<code>read [-1 -2 -4 -8 -s] [<i>count</i>] <i>offset</i></code> -1 Read byte value -2 Read 2 byte (short) value -4 Read 4 byte (int) value -8 Read 8 byte (long) value -s Read null-terminated string

Option	Description	Syntax
		<i>count</i> Number of values to read. If not specified, the default is 1 <i>offset</i> Disk offset to read. The value can be an expression as used by the <code>calculate</code> subcommand
<code>snapshot</code>	Sets the context of commands to the specified snapshot	<code>snapshot <i>snapshot_name</i></code>
<code>write</code>	Writes hexadecimal, octal, or decimal values at the disk offset, estimating how many bytes to write based on value size or number of digits in leading 0 hexadecimal values. The disk offset can be an expression used by the <code>calculate</code> subcommand. Numeric values can also be an expression as used by the <code>calculate</code> subcommand. This command is disabled in read-only mode.	<code>write [-1 -2 -4 -8 -c -s] [-C -CE] <i>offset value</i></code> -1 Write byte value -2 Write 2 byte (short) value -4 Write 4 byte (int) value -8 Write 8 byte (long) value -c Write text (no null termination). Enclose string in single-quotes (') -s Write null-terminated string. Enclose string in quotes (") -C Regenerate normal structure checksum -CE Regenerate extent structure checksum <i>offset</i> Disk offset to write. The value can be an expression used by the <code>calculate</code> subcommand <i>value</i> The value to write. If numeric, the value can be an expression as used by the <code>calculate</code> subcommand

Examples

[Example 78](#) shows the use of the `acfsdbg` subcommand.

Example 78 Using the `acfsdbg` command

```
$ /sbin/acfsdbg /dev/asm/volume1-123
acfsdbg: version = 11.2.0.3.0
Oracle ASM Cluster File System (ACFS) On-Disk Structure Version: 39.0
The ACFS volume was created at Mon Mar 2 14:57:45 2011
acfsdbg>

acfsdbg> calculate 60*1024
61,440
61440
61440
0xf000
0170000
1111:0000:0000:0000

acfsdbg> prompt "acfsdbg test>"
acfsdbg test>

echo "offset 64*1024" | acfsdbg /dev/asm/volume1-123
```

acfsutil info file

Purpose

Displays information for a file in an Oracle ACFS file system.

Syntax and Description

```
acfsutil info file -h
acfsutil info file [-d] [-o acfs_extent_offset] path
```

`acfsutil info file -h` displays help text and exits.

[Table 88](#) contains the options available with the `acfsutil info file` command.

Table 88 Options for the `acfsutil info file` command

Option	Description
<code>-d</code>	Displays detailed extent information, from Oracle ACFS to the Oracle ASM devices in the disk group.
<code>-o <i>acfs_extent_offset</i></code>	Narrows the extent display to the Oracle ACFS file offset specified.
<i>path</i>	Specifies the full path name of a file.

The `acfsutil info file` command displays information about a file in an Oracle ACFS file system. The information includes the extent map which details the locations of the blocks comprising the file and the used versus allocated storage for a file. Tagging information is also displayed for a file.

You must have read access to the specified file to run `acfsutil info file`.

Examples

The following is an example of `acfsutil info file`.

Example 79 Using the `acfsutil info file` command

```
$ /sbin/acfsutil info file /acfsmounts/acfs1/myfile
```

acfsutil info fs**Purpose**

Displays detailed Oracle ACFS file system information.

Syntax and Description

```
acfsutil info fs -h
acfsutil info fs [ {-o item | -s [interval [count]
                  [-d] ] | -f [-v] } ] [mount_point]
```

`acfsutil info fs -h` displays help text and exits.

[Table 89](#) contains the options available with the `acfsutil info fs` command.

Table 89 Options for the `acfsutil info fs` command

Option	Description
<code>-o</code>	Displays the specific file system item from the following list: <ul style="list-style-type: none"> <code>freespace</code> - Amount of free space available in the file system <code>totalspace</code> - Size of the file system <code>mountpoints</code> - Mount points associated with file systems. <code>volumes</code> - Number of volumes associated with the file system

Option	Description
	<ul style="list-style-type: none"> • <code>primaryvolume</code> - Path name of the device associated with file system • <code>available</code> - Length of time the file system has been available • <code>isadm</code> - 1 if an Oracle ADVM volume is present, 0 if not • <code>ismountpoint</code> - 1 if <code>path</code> is the mount point, 0 if <code>path</code> is not a mount point • <code>isavailable</code> - 1 if the file system is available, 0 if file system is not available • <code>iscorrupt</code> - 1 if the file system is corrupt, 0 if file system is not corrupt • <code>isreplprimary</code> - 1 if primary file system, 0 if not • <code>isreplstandby</code> - 1 if standby file system, 0 if not • <code>diskgroup</code> - Name of the disk group associated with <code>path</code> • <code>redundancy</code> - Type of redundancy used by the Oracle ADVM volume • <code>replication</code> - 1 if file system has been initialized for replication as the primary or standby file system, 0 if not initialized for replication • <code>resizeincrement</code> - Allocation unit size in bytes of the Oracle ADVM volume used by <code>path</code> • <code>stripewidth</code> - Stripe width for the Oracle ADVM volume used by <code>path</code> • <code>stripecolumns</code> - Stripe set columns for the Oracle ADVM volume used by <code>path</code> • <code>fetasize</code> - File entry table size which is the amount of storage consumed by the on disk metadata for inodes
<code>-s [interval [count] [-d]]</code>	<p>Displays file system statistics.</p> <p>The optional <code>interval</code> parameter specifies the amount of time in seconds between each report. The first report contains statistics for the time since the file system mount. Each subsequent report contains statistics collected during the interval since the previous report.</p> <p>The optional <code>count</code> parameter can be specified with the <code>interval</code> parameter. If the <code>count</code> parameter is specified, the value of count determines the number of reports generated at interval seconds apart.</p> <p>If the <code>interval</code> parameter is specified without the <code>count</code> parameter, the command generates reports continuously until you break out of the command with <code>Ctrl+c</code>.</p> <p>The optional <code>-d</code> option displays more detailed statistical information.</p>
<code>-f [-v]</code>	<p>Displays file system fragmentation. The <code>-v</code> option displays additional fragmentation information.</p>
<code>mount_point</code>	<p>Specifies the directory where the file system is mounted. Not a valid option for replication data.</p>

`acfsutil info fs` displays information and statistics about Oracle ACFS file systems. If replication has been initiated on a file system, additional flags and status information are displayed. The values for the **replication status** field are primary, standby, or disabled.

The `-o item` option displays file system information for the `item` specified.

The `-s` option displays the amount and rate of change currently on a file system for the node that the command is run on.

With no option specified, the command displays file system information that includes the volume device name, the size of the file system, the amount of space available on the volume device, the file system mount time on this node, the state of the file system, the user specified block size, the number of Oracle ACFS snapshots, the space consumed by snapshots in the file system, and the optional name or volume label associated with the file system. The possible file system states are displayed in the `flags` line. These states include:

- `Offline` indicates that the underlying devices are not accessible, possibly due to an Oracle ASM instance failure, disk group forced dismount, or an irrecoverable I/O error. The file system on this node can only be dismounted. All other attempts at access result in errors.
- `Available` indicates that the file system is on line and operational.
- `Corrupt` indicates that the file system should be checked and repaired at the earliest possible convenience to correct a detected inconsistency. For example, run the `fsck` command on Linux or the `acfschkdsk` command on Windows to check and repair the file system. Ensure that you run the command in repair mode to correct the problem. For more information, refer to “[fsck](#)” and “[acfschkdsk](#)”.

When viewing space usage values with `acfsutil info fs` on Windows systems, the values may differ from sizes in Windows folders. The mechanism used by **Folder Properties** on Windows systems only accounts for files and should be considered an approximate value.

Any user can run `acfsutil info fs`.

Examples

The following are examples of the use of `acfsutil info fs`.

[Example 80](#) displays information about an Oracle ACFS file system in a Linux environment.

Example 80 Using the `acfsutil info fs` command on Linux

```
$ /sbin/acfsutil info fs
/primary
  ACFS Version: 11.2.0.2.0
  flags:       MountPoint,Available,Replication
  mount time:  Mon Oct 25 12:11:03 2010
  volumes:    1
  total size:  5368709120
  total free:  4144230400
  primary volume: /dev/asm/pvol-74
    label:
    flags:           Primary,Available,ADVM
    on-disk version: 40.0
    allocation unit: 4096
    major, minor:   252, 37889
    size:           5368709120
    free:          4144230400
    ADVM diskgroup  REPLDG
    ADVM resize increment: 268435456
    ADVM redundancy: unprotected
    ADVM stripe columns: 4
    ADVM stripe width: 131072
  number of snapshots: 0
  snapshot space usage: 0
```

```

replication status: primary

/standby
ACFS Version: 11.2.0.2.0
flags:      MountPoint,Available,Replication
mount time: Mon Oct 25 12:11:03 2010
volumes:   1
total size: 5368709120
total free: 5263945728
primary volume: /dev/asm/svol-74
  label:
  flags:      Primary,Available,ADVM
  on-disk version: 40.0
  allocation unit: 4096
  major, minor: 252, 37890
  size:      5368709120
  free:     5263945728
  ADVM diskgroup REPLDG
  ADVM resize increment: 268435456
  ADVM redundancy: unprotected
  ADVM stripe columns: 4
  ADVM stripe width: 131072
number of snapshots: 0
snapshot space usage: 0
replication status: standby

```

```

$ /sbin/acfsutil info fs -o mountpoints,replication
/primary
1
/standby
1

```

```

$ /sbin/acfsutil info fs -o mountpoints,isreplprimary
/primary
1
/standby
0

```

```

$ /sbin/acfsutil info fs -o mountpoints,isreplstandby
/primary
0
/standby
1

```

[Example 81](#) illustrates the use of `acfsutil info fs` in a Windows environment.

Example 81 Using the `acfsutil info fs` command on Windows

```

C:\oracle>acfsutil info fs /o freespace c:\oracle\acfsmounts\acfs1
968667136

C:\oracle>acfsutil info fs /o totalspace c:\oracle\acfsmounts\acfs1
1073741824

C:\oracle>acfsutil info fs /o volume c:\oracle\acfsmounts\acfs1
1

C:\oracle>acfsutil info fs /o primaryvolume c:\oracle\acfsmounts\acfs1
asm-volumel-311

C:\oracle>acfsutil info fs /o diskgroup c:\oracle\acfsmounts\acfs1
DATA

C:\oracle>acfsutil info fs /o redundancy c:\oracle\acfsmounts\acfs1
mirror

```

[Example 82](#) illustrates the use of `acfsutil info fs` with `-s` option to display the current amount and rate of change on a file system.

Example 82 Using the `acfsutil info fs` command with the `-s` option

```
$ /sbin/acfsutil info fs -s /acfsmounts/acfs1
  amount of change since mount:      359.22 MB
  average rate of change since mount: 3 KB

$ /sbin/acfsutil info fs -s 60 4 /acfsmounts/acfs1
  amount of change since mount:      359.22 MB
  average rate of change since mount: 3 KB/s

  amount of change: 15.02 MB   rate of change: 256 KB/s
  amount of change: 9.46 MB   rate of change: 161 KB/s
  amount of change: 7.32 MB   rate of change: 125 KB/s
  amount of change: 6.89 MB   rate of change: 117 KB/s
...
```

acfsutil info id

Purpose

Displays Oracle ACFS file system information for a specified file identifier number and mount point.

Syntax and Description

```
acfsutil info id -h
acfsutil info id file_identifier mount_point
```

`acfsutil info id -h` displays help text and exits.

[Table 90](#) contains the options available with the `acfsutil info id` command.

Table 90 Options for the `acfsutil info id` command

Option	Description
<i>mount_point</i>	Specifies the directory where the file system is mounted.
<i>file_identifier</i>	Specifies the Oracle ACFS file identifier number reported by the Oracle ACFS driver. The file identifier number should be specified in decimal format.

You can use `acfsutil info id` to translate an internal numeric Oracle ACFS file identifier to a path name in the file system. This is useful when the Oracle ACFS driver reports I/O errors to the system event logger associated with a particular file in an Oracle ACFS and identifies it by its internal identifier. You must have administrator privileges or you must be a member of the Oracle ASM administrator group to run `acfsutil info id`.

Examples

The following is an example of `acfsutil info id`.

Example 83 Using the `acfsutil info id` command

```
$ /sbin/acfsutil info id 117 /acfsmounts/acfs1
```

acfsutil plugin disable

Purpose

Disables the Oracle ACFS plug-in infrastructure for an Oracle ACFS file system.

Syntax and Description

```
acfsutil plugin disable -h
acfsutil plugin disable mount_point
```

`acfsutil plugin disable -h` displays help text and exits.

[Table 91](#) contains the options available with the `acfsutil plugin disable` command.

Table 91 Options for the `acfsutil plugin disable` command

Option	Description
<code>mount_point</code>	Specifies the directory where the file system is mounted.

`acfsutil plugin disable` disables the collection of Oracle ACFS plug-in metrics and the associated communication with a plug-in application.

Administrator privileges are required to use this command or you must be a member of the Oracle ASM administrator group.

Examples

[Example 84](#) shows the use of the `acfsutil plugin disable` command. After monitoring has completed for the Oracle ACFS file metric data for the file system mounted on the `/humanresources`, the command in [Example 84](#) disables the subsequent collection of summary data in the Oracle ACFS driver.

Example 84 Disabling the Oracle ACFS driver

```
# /sbin/acfsutil plugin disable /humanresource
```

acfsutil plugin enable

Purpose

Enables the Oracle ACFS plug-in infrastructure for an Oracle ACFS file system.

Syntax and Description

```
acfsutil plugin enable -h
acfsutil plugin enable -m metrictype [-t tag, ...]
                        [-i interval[s|m]] mount_point
```

`acfsutil plugin enable -h` displays help text and exits.

[Table 92](#) contains the options available with the `acfsutil plugin enable` command.

Table 92 Options for the `acfsutil plugin enable` command

Option	Description
<code>-t tag, ...</code>	An optional list of tag names selecting Oracle ACFS files that you want to be monitored. The maximum number of tags is 12. The names are separated by commas. The default is to monitor all files in the Oracle ACFS file system.
<code>-m metrictype</code>	Selects the message payload to be transmitted from Oracle ACFS to the plug-in module with each call-out message. Oracle ACFS provides the <code>acfsmetric1</code> pre-defined metric type.
<code>-i interval [s m]</code>	Selects posting message delivery and the posting interval. The Oracle ACFS plug-in mechanism posts a metrics message during each specified message interval. An interval is the maximum amount of time which can pass before metrics are posted. The application blocks in the API call to retrieve metrics until a posting occurs. The interval can be specified as an integer value in <code>s</code> seconds or <code>m</code> minutes. The default is minutes. The maximum value allowed for an interval is 60 minutes or 3600 seconds. If an interval is specified, then Oracle ACFS is requested to post metrics messages to the plug-in application on an interval basis. If an interval is not specified, then the application polls for metrics updates from the Oracle ACFS file system. This is the default action.
<code>mount_point</code>	Specifies the directory where the file system is mounted.

`acfsutil plugin enable` enables an Oracle ACFS file system for application plug-in service. Oracle ACFS plug-ins are enabled for single nodes only, either a standalone host or one or more individual nodes of a Grid Cluster. After enabled for plug-ins, the Oracle ACFS file system begins collecting metric information for either the set of specified tagged files or all files in the Oracle ACFS file system, and transmits callout messages to the plug-in application based upon the selected message payload and delivery parameters. Metrics are reset after every delivery to the application (whether through polling or posting).

In general, metrics are collected from the point of view of a user application. I/O for metadata or internal Oracle ACFS activities; such as snapshot copy-on-writing, encrypting, and replicating files; are not included. Metrics are collected for user I/O to both files in the original file system and snapshot files. Memory mapping of files that results in I/O operations is recorded in the metrics. Replication related files under the `.ACFS/repl` directory are not included in the metrics.

Oracle ACFS provides the `acfsmetric1` pre-defined metric type. For information about the pre-defined metric types, refer to “[Oracle ACFS Pre-defined Metric Types](#)”.

Administrator privileges are required to use this command or you must be a member of the Oracle ASM administrator group.

Examples

[Example 85](#) shows the use of the `acfsutil plugin enable` command to provide additional storage usage metrics to a monitoring application.

Example 85 Enabling the Oracle ACFS driver for storage visibility: poll model

```
# /sbin/acfsutil plugin enable -m acfsmetric1 -t HRDATA /humanresource
```

An Oracle ACFS file system mounted on `/humanresources` is to be enabled for plug-in service and configured with the objective of providing additional storage usage metrics to a monitoring application. The message payload type is `acfsmetric1`, the files to be monitored are human resource files that have been tagged with the Oracle ACFS file tag `HRDATA`, and the message delivery type is `poll` which means that the application plug-in polls to request metric data update messages. No interval is specified with polled message delivery.

When the command in [Example 85](#) completes, the Oracle ACFS file system mounted on the `/humanresources` mount point is enabled for plug-in communication and begins collecting Oracle ACFS file access metrics for files tagged with `HRDATA`. Oracle ACFS maintains metrics collecting a summary of read and write activity. Each time the associated application plug-in module polls for the metrics, Oracle ACFS sends a message with the data as defined in the `ACFS_METRIC1` structure that is a summary of the selected Oracle ACFS activity since either the Oracle ACFS driver plug-in functionality was enabled or since the last delivery of metric data.

[Example 86](#) shows the use of the `acfsutil plugin enable` command to monitor movie file updates.

Example 86 Enabling the Oracle ACFS driver for storage visibility: post on interval model

```
# /sbin/acfsutil plugin enable -m acfsmetric1 -t FILECONTENT -i 120s /moviemods
```

An Oracle ACFS file system mounted on `/moviemods` is enabled for plug-in service and is configured to record and deliver storage usage messages to a monitoring application. On an interval basis, the Oracle ACFS file system sends a wakeup on a driver event on which the application API call is waiting. The application then collects a summary of read and write activity on the files.

The message payload type is `acfsmetric1` and the files to be monitored are movie files that have been tagged with the `FILECONTENT` tag. The message delivery type is `post`, which means that Oracle ACFS posts messages containing the metrics to the plug-in application for the specified interval of 120 seconds.

When the command in [Example 86](#) completes, the Oracle ACFS file system mounted on the `/moviemods` mount point is enabled for plug-in communication and begins collecting Oracle ACFS storage visibility metrics for files tagged with `FILECONTENT`. On each interval, Oracle ACFS posts one or more messages to the application plug-in containing the storage visibility information.

acfsutil plugin info

Purpose

Displays information about the Oracle ACFS plug-in infrastructure for an Oracle ACFS file system.

Syntax and Description

```
acfsutil plugin info -h  
acfsutil plugin info mount_point
```

`acfsutil plugin info -h` displays help text and exits.

[Table 93](#) contains the options available with the `acfsutil plugin info` command.

Table 93 Options for the `acfsutil plugin info` command

Option	Description
<code>mount_point</code>	Specifies the directory where the file system is mounted.

`acfsutil plugin info` displays information about the state of the Oracle ACFS plug-in mechanism.

Administrator privileges are required to use this command or you must be a member of the Oracle ASM administrator group.

Examples

[Example 87](#) shows the use of the `acfsutil plugin info` command.

Example 87 Displaying information about the Oracle ACFS driver

```
# /sbin/acfsutil plugin info /humanresource

Plug-in status: ENABLED
Metric type: acfsmetric1
Enabled tags: HRDATA
Delivery method: Poll
Post interval (seconds):

# /sbin/acfsutil plugin info /moviemods

Plug-in status: ENABLED
Metric type: acfsmetric1
Enabled tags: FILECONTENT
Delivery method: Post
Post interval (seconds): 120
```

acfsutil registry

Purpose

Adds, deletes, or displays entries in the Oracle ACFS mount registry.

Syntax and Description

```
acfsutil registry -h
acfsutil registry
acfsutil registry -a [-f] [-o moptions] [-n { nodes|all } ]
    [-u user] [-t description] device mount_point
acfsutil registry -c {device | mount_point} [-o moptions]
    [-n { nodes|all } ] [-u user] [-t description]
acfsutil registry -d {device | mount_point}
acfsutil registry -l [device | mount_point]
acfsutil registry -m deviceacfsutil registry -r
```

`acfsutil registry -h` displays help text and exits.

If no options are specified, the command displays all the Oracle ACFS file systems that are configured for automatic start.

[Table 94](#) contains the options available with the `acfsutil registry` command.

Table 94 Options for the *acfsutil* registry command

Option	Description
-a	Add the device, mount point, and associated <i>options</i> to the Oracle ACFS mount registry. The Oracle ADVM volume device specified must exist on the local node to add the information to the mount registry. The arguments represent all the information needed to mount the file system. At Oracle ACFS startup time these file systems are automatically mounted. Duplicate device entries are not allowed. Duplicate mount points are allowed but must include the -n option for disjoint node-specific mounts.
-c	Changes an existing registry entry for the specified device or mount point.
-d	Deletes the specified device or mount point from the Oracle ACFS mount registry. If a mount point is specified and it is not unique in the Oracle ACFS mount registry, the command fails and you must run the command again specifying the device.
-f	This option is used in combination with -a when the specified device might exist in the registry and the administrator wants to replace the registration.
-l [<i>device</i> <i>mount_point</i>]	Without specifying a device or mount point, the -l option lists all the file systems currently in the registry on a single line, with fields separated by a colon (:). With a device specified, lists information about the device in the Oracle ACFS registry. With a mount point specified, lists information about the mount point in the Oracle ACFS registry.
-m <i>device</i>	Lists the registered mount point, if one exists, associated with the specified device. The mount point is only returned if the Oracle ACFS file system has been registered or has been previously mounted.
-n { <i>nodes</i> all }	This option, used in combination with -a and -c, specifies an optional comma-delimited list of nodes, or the all keyword. This specifies which nodes should attempt to mount this device on the specified mount point. Host names should be specified. The all keyword is functionally equivalent to not specifying a list of nodes and indicates that the device should be mounted on all nodes. Mounting on all nodes is the default behavior.
-o <i>options</i>	Specifies the mount options for use when mounting the file system. Valid for Linux, Solaris, and AIX. Used in combination with -a and -c. For specific -o <i>options</i> , refer to the mount command for each operating system. All the options for each operating system are available except the all option.
-r	Displays all registered file systems, not just file systems with auto_start=always.
-t <i>description</i>	Adds a description of the mount. Used in combination with -a and -c. For example: -t "HR Exports share". This description can be seen later when looking at configured resources.
-u <i>user</i>	Specifies a user that is allowed to mount or umount (start and stop) the file system. This option, used in combination with -a and -c, is useful for creating a registered file system that can be started or stopped by someone other than root.

Option	Description
<i>mount_point</i>	Specifies the directory where the file system is mounted.
<i>device</i>	Specifies an Oracle ACFS device file that has been formatted.

`acfsutil registry` adds, deletes, or displays a file system from the Oracle ACFS persistent mount registry. The mount registry is a global registry that is used at Oracle ACFS startup on each node to mount all file systems specified in it. `root` or `asmadmin` privileges are required to modify the registry. For information about operating system group privileges, see “[About Privileges for Oracle ASM](#)”.

Any user is allowed to display the contents of the registry. To mount all the file systems in the Oracle ACFS mount registry, use the platform specific mount command with the `all` option. This is done automatically at Oracle ACFS startup on each node.

Note:

Oracle ACFS registration (`acfsutil registry`) is not supported in an Oracle Restart (standalone) configuration, which is a single-instance (non-clustered) environment.

See “[About the Oracle ACFS Mount Registry](#)”.

Examples

The following examples show the use of `acfsutil registry`. The first example shows how to add the volume device file and file system mount point to the registry. The second example shows how to list the registered mount point associated with the specified volume device file. The third example shows how to delete the specified volume device file from the registry.

Example 88 Using the `acfsutil registry` command

```
$ /sbin/acfsutil registry -a /dev/asm/volume1-123 /acfsmounts/acfs1
$ /sbin/acfsutil registry -m /dev/asm/volume1-123
$ /sbin/acfsutil registry -d /dev/asm/volume1-123
```

acfsutil rmfs

Purpose

Removes an Oracle ACFS file system.

Syntax and Description

```
acfsutil rmfs -h
acfsutil rmfs device
acfsutil rmfs device -b
```

`acfsutil rmfs -h` displays help text and exits.

[Table 95](#) contains the options available with the `acfsutil rmfs` command.

Table 95 Options for the `acfsutil rmfs` command

Option	Description
<code>device</code>	Specifies an Oracle ACFS device file that has been formatted.
<code>-b</code>	Specifies batch mode. No user interaction is required.

You can use `acfsutil rmfs` to remove an Oracle ACFS that is dismounted. When the command is run, the superblock of the file system is disabled. `root` or `asmadmin` privileges are required to run this command. For information about operating system group privileges, see [“About Privileges for Oracle ASM”](#).

After `acfsutil rmfs` runs successfully, the `MOUNTPATH` and `USAGE` columns in the `V $ASM_VOLUME` view are cleared for the device. The removed Oracle ACFS can be restored using `fsck` or `acfschkdsk`. The device can be reformatted with a new Oracle ACFS using the `mkfs` or `acfsformat` commands.

Examples

The following example shows the use of `acfsutil rmfs` to remove the specified volume device file and associated file system.

Example 89 Using the `acfsutil rmfs` command

```
$ /sbin/acfsutil rmfs /dev/asm/volume1-123
```

acfsutil size

Purpose

Resizes an Oracle ACFS file system.

Syntax and Description

```
acfsutil size -h
acfsutil size [+|-]n[K|M|G|T|P ] mount_point
```

`acfsutil size -h` displays help text and exits.

[Table 96](#) contains the options available with the `acfsutil size` command.

Table 96 Options for the `acfsutil size` command

Option	Description
<code>[+ -]n</code>	Specifies the new size for the Oracle ACFS file system where <code>n</code> is a valid positive whole number greater than zero. The number can be preceded by a <code>+</code> or <code>-</code> to indicate the amount to add or decrease. If no operand exists, the new size is the absolute size.
<code>K M G T P</code>	Specifies that the integer supplied for size is in the units of <code>K</code> (Kilobytes), <code>M</code> (Megabytes), <code>G</code> (Gigabytes), <code>T</code> (Terabytes), or <code>P</code> (Petabytes). If the unit indicator is specified, then it must be appended to the integer. If omitted, the default unit is bytes.
<code>mount_point</code>	Specifies the directory where the file system is mounted

`acfsutil size` grows or shrinks the mounted Oracle ACFS and its underlying Oracle ADVM storage to match the new size specified. This operation also resizes the underlying Oracle ADVM volume file to match the new length that is specified.

However, the disk group must have enough free storage to accommodate any requested increase to the file system size.

Reducing a file system size returns unused storage space located at the end of the file system to the disk group. Shrinking in this release is intended for accidents when the wrong initial size or resize increment was specified, and before the storage was actually used. After storage has been used for user data or file system metadata, it may not be possible to shrink the file system, even if the files using that storage have been deleted.

Note:

Defragmenting a file system is not supported in this release; only unused storage can be deallocated from the end of the file system.

The size value is rounded up based on the block size of the file system and the allocation unit of the Oracle ADVM volume device file. To determine the Oracle ADVM volume device resize increment, examine the `RESIZE_UNIT_MB` field in the `V $ASM_VOLUME` view, `Resize Unit` in the output of `asmcmd volinfo`, or `ADVM resize increment` in the output of `acfsutil info fs`.

There is no limit to the number of times a file system can be expanded for a disk group with the ADVM compatibility attribute set to `11.2.0.4` or higher.

For a disk group with the ADVM compatibility attribute set to less than `11.2.0.4`, there is a limit of 5 extents for the file system's internal storage bitmap. This causes any attempts to increase the file system to fail after it has been increased four or more times. However, if after increasing the file system four times or more times the file system size is decreased, then you may be able to increase the file system size again if the size of the increase is less than the size of the decrease. When the limit on a file system expansion has been reached, running `fsck` or `acfschkdsk` with the `-a` option may consolidate the internal storage bitmap, allowing future file system expansion.

`root` or users who are members of the `asmadmin` group can run this command. For information about operating system group privileges, see [“About Privileges for Oracle ASM”](#).

Examples

The following example shows the use of `acfsutil size`. This example increases the primary device file of `/acfsmounts/acfs1` file system by 500 MB.

Example 90 Using the `acfsutil size` command

```
$ /sbin/acfsutil size +500M /acfsmounts/acfs1
```

acfsutil snap convert

Purpose

Converts the type of an existing snapshot image from read-only to read-write or read-write to read-only.

Syntax and Description

```
acfsutil snap convert -h
acfsutil snap convert [-r|-w] snapshot mount_point
```

`acfsutil snap convert -h` displays help text and exits.

[Table 97](#) contains the options available with the `acfsutil snap convert` command.

Table 97 Options for the `acfsutil snap convert` command

Option	Description
<code>-r</code>	Converts snapshot to read-only snapshot.
<code>-w</code>	Converts snapshot to read-write snapshot.
<code>snapshot</code>	Specifies the name of the snapshot to be converted.
<code>mount_point</code>	Specifies the directory where the file system is mounted.

`acfsutil snap convert` converts the type of an existing snapshot image from a read-only snapshot image to a read-write snapshot image, or from a read-write snapshot image to a read-only snapshot image.

The type option (`-r` or `-w`) is required for the convert operation. Specifying a type parameter that matches the type of the existing snapshot image results in no conversion and no failure. An 11.2 read-only snapshot image can be converted to a read-write snapshot image, but this conversion results in an update of the Oracle ACFS on-disk structure version. After the Oracle ACFS on-disk structure version has been updated, the updated version is not compatible with previous Oracle ACFS 11.2 versions.

Administrator privileges are required to use this command or you must be a member of the Oracle ASM administrator group.

Examples

[Example 91](#) shows the use of the `acfsutil snap convert` command.

Example 91 Using the `acfsutil snap convert` command

```
$ acfsutil snap convert -w midday_test1 /acfsmounts/critical_apps
$ acfsutil snap convert -r midday_test2 /acfsmounts/critical_apps
```

acfsutil snap create

Purpose

Creates a read-only or read-write snapshot of an Oracle ACFS file system or an existing snapshot.

Syntax and Description

```
acfsutil snap create -h
acfsutil snap create [-r|-w] [-p parent_snapshot] snapshot mount_point
```

`acfsutil snap create -h` displays help text and exits.

[Table 98](#) contains the options available with the `acfsutil snap create` command.

Table 98 Options for the `acfsutil snap create` command

Option	Description
<code>-r</code>	Creates a read-only snapshot. This is the default setting.

Option	Description
<code>-w</code>	Creates a read-write snapshot.
<code>snapshot</code>	Specifies a name for the snapshot. The name provided must be a valid directory name. The <code>.ACFS/snaps</code> directory itself cannot be snapped.
<code>-p parent_snapshot</code>	Specifies the name of an existing snapshot image within the Oracle ACFS file system.
<code>mount_point</code>	Specifies the directory where the file system is mounted.

`acfsutil snap create` creates a read-only or read-write snapshot of the Oracle ACFS file system mounted on `mount_point` or creates a snapshot of an existing snapshot if the `-p` option is specified. You can specify `-r` for read-only or `-w` for read-write; read-only is the default if neither `-r` or `-w` are specified.

The read-write snapshot enables the fast creation of an Oracle ACFS snapshot image that can be both read and written without impacting the state of the Oracle ACFS file system hosting the snapshot images. You can use the read-write functionality for testing new versions of application software or running test scenarios on production file data without modifying the original file system.

Snapshots are not separate file systems. The snapshot appears in the `.ACFS/snaps/snapshot` directory and initially is a complete replica of the file system at the time the snapshot command was given. A read-only snapshot continues to preserve that initial point-in-time view. A read-write snapshot can be modified by updates written directly to the files located within the `.ACFS/snaps/snapshot` hierarchy.

A symbol link (symlink) file is a pointer to a path specified at the time that the symlink is created. For any existing symlink in the source of the `acfsutil snap create` command, a new link is made in the snapshot; however, the stored path to the symlink target is not modified during snap creation time. When an absolute path is used as the target of the link, the link target of the snapshot still refers to the absolute path, outside the newly-created snapshot namespace. Future modifications to the targeted file can occur through the snapshot symlink, not to a new target inside the snapshot namespace. The contents of the targeted file can also be changed outside of the snapshot. Because of this behavior, you should use relative path targets for all symlinks that are within the same file system.

Any user can access the snapshot directory by specifying the path name. However, the `.ACFS` directory itself is hidden from directory listings of the root of the file system. This prevents recursive commands, such as `rm -rf` or `acfsutil tag set -r`, from the root of the file system inadvertently operating on snapshot files.

Snapshots usually use very little storage initially as they share file system blocks with the original file system until a file changes.

Tools such as `du` report the total disk space usage of the snapshotted files, which includes the storage shared with the original versions of the files. To determine the total space used for the snapshots, use the `acfsutil snap info` or `acfsutil info fs` command. See “[acfsutil info fs](#)”.

Oracle ACFS snapshots are immediately available for use after they are created. They are always online under the `.ACFS/snaps` directory when the original file system is mounted. No separate command is needed to mount them.

The `acfsutil snap create` operation fails if the cluster is in rolling migration.

Creation from an existing snapshot is not permitted if there are:

- Any snapshots present in the file system that were created with the ADVN compatibility set to less than 12.1
- Any snapshots of the file system that were created after ADVN compatibility was set to 12.1 but while 11.2 snapshots existed
- Any snapshot deletion cleanup operations still running in the background for the above conditions

You can display pending snapshot operations with the `acfsutil snap info` command. For information, refer to “[acfsutil snap info](#)”.

Administrator privileges are required to use this command or you must be a member of the Oracle ASM administrator group.

For more information about Oracle ACFS snapshots, refer to “[About Oracle ACFS Snapshots](#)”. For information about the number of snapshots supported, refer to “[Oracle ACFS Disk Space Usage](#)”.

Examples

[Example 92](#) shows the use of the `acfsutil snap create` command to create snapshots on a Linux platform.

Example 92 Using the `acfsutil snap create` command on Linux

```
$ acfsutil snap create -w midday_test1 /acfsmounts/critical_apps
$ acfsutil snap create -w midday_test2 /acfsmounts/critical_apps
$ /sbin/acfsutil snap create payroll_report1 /acfsmounts/critical_apps
$ /sbin/acfsutil snap create payroll_report2 /acfsmounts/critical_apps
$ ls /acfsmounts/critical_apps/.ACFS/snaps
midday_test1 midday_test2 payroll_report1 payroll_report2
```

[Example 93](#) shows the use of the `acfsutil snap create` command to create snapshots on a Windows platform. This example shows the creation of a snapshot from an existing snapshot.

Example 93 Using the `acfsutil snap create` command on Windows

```
$ /sbin/acfsutil snap create /w snap_1 e:
$ /sbin/acfsutil snap create /w snap_1-1 /p snap_1 e:
```

acfsutil snap delete

Purpose

Deletes a snapshot of an Oracle ACFS file system.

Syntax and Description

```
acfsutil snap delete -h
acfsutil snap delete snapshot mount_point
```

`acfsutil snap delete -h` displays help text and exits.

[Table 99](#) contains the options available with the `acfsutil snap delete` command.

Table 99 Options for the `acfsutil snap delete` command

Option	Description
<code>snapshot</code>	Specifies a name for the snapshot.
<code>mount_point</code>	Specifies the directory where the file system is mounted.

`acfsutil snap delete` deletes the snapshot named `snapshot` in the Oracle ACFS mounted on `mount_point`. After successful completion of the command, the representation of the snapshot in the `.ACFS/snaps` directory is removed. The command fails if any file within the snapshot is open on any cluster node. The disk space used by the snapshot being deleted is freed by a background task after the completion of the `acfsutil snap delete` command. If one of these background threads is running to clean up a deleted snapshot, then the `acfsutil snap info` command shows a pending delete operation. For information about the `acfsutil snap info` command, refer to “[acfsutil snap info](#)”.

The `acfsutil snap delete` operation fails if the cluster is in rolling migration

Administrator privileges are required to use this command or you must be a member of the Oracle ASM administrator group.

Examples

[Example 94](#) shows the use of the `acfsutil snap delete` command.

Example 94 Using the `acfsutil snap delete` command

```
$ /sbin/acfsutil snap delete midday_test1 /acfsmounts/critical_apps
acfsutil snap delete: Snapshot operation is complete.
```

acfsutil snap info

Purpose

Displays information about Oracle ACFS file system snapshots.

Syntax and Description

```
acfsutil snap info -h
acfsutil snap info -t [snapshot] mount_point
```

`acfsutil snap info -h` displays help text and exits.

[Table 100](#) contains the options available with the `acfsutil snap info` command.

Table 100 Options for the `acfsutil snap info` command

Option	Description
<code>-t</code>	Displays a tree structure for the specified snapshot and mount point.
<code>snapshot</code>	Specifies a name for the snapshot.
<code>mount_point</code>	Specifies the directory where the file system is mounted.

The `acfsutil snap info` command displays information about an individual specified snapshot or all snapshots in the specified Oracle ACFS file system. The snapshot name, snapshot type (RO or RW), parent name, creation date and time, and

space used are displayed. The parent name is either the mount point, or the parent snapshot if the snapshot was created from an existing snapshot.

The snapshot space usage amount includes snapshot metadata. If all the files are deleted from a snapshot, some metadata still remains and that amount is displayed with `acfsutil snap info`.

To reclaim the disk space used by snapshots, delete the snapshots. Deleting the files within the snapshots may not reclaim this disk space.

The `acfsutil snap info` command also shows pending delete operations.

Oracle ACFS caches and asynchronously updates snapshot storage usage statistics. If an Oracle ASM instance is killed, power is lost to the machine, or the Oracle ACFS file system goes offline for any reason, one of these cached updates may be lost. This loss can result in the display of a message similar to `Reported snapshot space usage is inaccurate when acfsutil snap info is run`.

Examples

[Example 95](#) shows the use of the `acfsutil snap info` command on a Linux platform when there is a pending delete operation. When the background process finishes the clean up of the deleted snapshot, the delete pending row does not appear in the output.

Example 95 Using the `acfsutil snap info` command on Linux

```
$ /sbin/acfsutil snap info /acfsmounts/critical_apps
snapshot name:          midday_test2
RO snapshot or RW snapshot: RW
parent name:           /acfsmounts/critical_apps
snapshot creation time:  Fri Feb 18 06:10:59 2011

snapshot name:          payroll_report1
RO snapshot or RW snapshot: RO
parent name:           /acfsmounts/critical_apps
snapshot creation time:  Tue Feb 22 06:56:34 2011

snapshot name:          payroll_report2
RO snapshot or RW snapshot: RO
parent name:           /acfsmounts/critical_apps
snapshot creation time:  Tue Feb 22 06:57:21 2011

    number of snapshots:  3 (active)
                        1 (delete pending)
snapshot space usage: 8383348736
```

[Example 96](#) shows the use of the `acfsutil snap info` command on a Windows platform. These commands were run after the `acfsutil snap create` commands in [Example 93](#).

Example 96 Using the `acfsutil snap info` command on Windows

```
$ /sbin/acfsutil snap info e:

snapshot name:          snap_1
RO snapshot or RW snapshot: RW
parent name:           e:
snapshot creation time:  Thu Oct 13 13:24:52 2011

snapshot name:          snap_1-1
RO snapshot or RW snapshot: RW
parent name:           snap_1
snapshot creation time:  Thu Oct 13 13:30:31 2011
```



```

    number of snapshots: 2
    snapshot space usage: 65536

$ /sbin/acfsutil snap info /t e:

e:                RW
snap_1            RW   e:
snap_1-1          RW   snap_1

$ /sbin/acfsutil snap info /t snap1 e:

snap_1            RW
snap_1-1          RW   snap_1

```

acfsutil tune

Purpose

The `acfsutil tune` command displays the value of a specific tunable parameter or all Oracle ACFS tunable parameters, or sets the value of a tunable parameter in a persistent manner on a particular node.

Syntax and Description

```

acfsutil tune -h
acfsutil tune [tunable_name]
acfsutil tune tunable_name=value

```

`acfsutil tune -h` displays help text and exits.

[Table 101](#) contains the options available with the `acfsutil tune` command.

Table 101 Options for the `acfsutil tune` command

Option	Description
<i>tunable_name</i>	Specifies the name of the tunable parameter.
<i>value</i>	Specifies the value for a tunable parameter.

The Oracle ACFS tunable parameter `AcfsMaxOpenFiles` limits the number of open Oracle ACFS files on Windows and AIX. Normally you do not have to change the value of this tunable parameter; however, you may want to consider increasing the value if you have a large working set of files in your Oracle ACFS file systems.

The Oracle ACFS tunable parameter `AcfsMaxCachedFiles` sets the maximum number of closed files that remain cached in memory on Windows and AIX. Normally you do not have to change value of this tunable parameter; however, you many to consider changing the value to get better performance.

Changing a tunable parameter has an immediate effect and persists across restarts. You must be a root user or the Windows Administrator to change the value of a tunable parameter.

Examples

The first command prints Oracle ACFS tunable parameters. The second command changes the value of a tunable parameter.

Example 97 Using the acfsutil tune command

```
$ /sbin/acfsutil tune
$ acfsutil tune AcfsMaxOpenFiles=50000
```

advmutil canonical**Purpose**

`advmutil canonical` displays the canonical name of the specified Oracle ADVM device name.

Syntax and Description

```
advmutil -h
advmutil canonical volume_device
```

`advmutil -h` displays help text and exits.

[Table 102](#) contains the options available with the `advmutil canonical` command.

Table 102 Options for the advmutil canonical command

Option	Description
<i>volume_device</i>	Specifies a string identifying an Oracle ADVM volume device.

There are several different formats that can identify an Oracle ADVM volume device, but a normalized, unambiguous (canonical) name should be used when the volume device name is used with other commands such as `SRVCTL`.

For example, on the Windows operating system you can use the following prefixes with a volume device name: `\\. \, \??\, \\?\`

The `advmutil canonical` command would return the canonical name that another utility would recognize without having to strip off extra characters. The command would most likely be used in a script.

Examples

The following examples show the use of `advmutil canonical` on a Windows operating system. For each example, the command returns the canonical name of the volume device.

Example 98 Using advmutil canonical

```
[C:\]advmutil canonical asm-volume1-274
asm-volume1-274

[C:\]advmutil canonical \\. \asm-volume1-274
asm-volume1-274

[C:\]advmutil canonical \\?\asm-volume1-274
asm-volume1-274

[C:\]advmutil canonical \??\asm-volume1-274
asm-volume1-274
```

advmutil tune

Purpose

`advmutil tune` displays the value of a specific Oracle ADVM parameter or sets the value of a specific Oracle ADVM parameter.

Syntax and Description

```
advmutil -h
advmutil tune parameter [= value]
```

`advmutil -h` displays help text and exits.

[Table 103](#) contains the options available with the `advmutil tune` command.

Table 103 Options for the `advmutil tune` command

Option	Description
<i>parameter</i>	Specifies the parameter for which you want to set or display the value.
<i>value</i>	Optional value provided to set the value of the specified parameter.

If a value is not provided, the `advmutil tune` command displays the value that is currently assigned to the specified parameter.

The parameter that can be specified with `advmutil tune` is the maximum time in minutes for the deadlock timer (`deadlock_timer`).

You must be a privileged user to set a parameter.

Note:

The `deadlock_timer` parameter should only be set by Oracle Support Services.

Examples

The first example changes the maximum time in minutes for the deadlock timer. The second example queries the current setting of a parameter.

Example 99 Using `advmutil tune`

```
$ /sbin/advmutil tune deadlock_timer = 20

$ /sbin/advmutil tune deadlock_timer
deadlock_timer = 20 (0x14)
```

advmutil volinfo

Purpose

`advmutil volinfo` displays information about Oracle ADVM volume devices.

Syntax and Description

```
advmutil -h
advmutil volinfo [-l][-L] [volume_device]
```

advmutil -h displays help text and exits.

Table 104 contains the options available with the advmutil volinfo command.

Table 104 Options for the advmutil volinfo command

Option	Description
<i>volume_device</i>	Specifies an optional volume device name.
-l	Separates the Oracle ADVM volume device information by field descriptions and colons on one line.
-L	Separates the Oracle ADVM volume device information by spaces on one line.

advmutil volinfo displays information about Oracle ADVM volume devices in a list format by default. The -l option on Linux (/l on Windows) formats the display into a colon-separated string with field descriptions. The -L option on Linux (/L on Windows) formats the display into a space-separated string in a format suitable for scripting.

Examples

The first example displays information about an Oracle ADVM volume device, using the advmutil volinfo command with the volume device name. The second example displays information about the volume device using the -l option. The third example displays information about the volume device using the -L option.

Example 100 Using advmutil volinfo

```
$ /sbin/advmutil volinfo /dev/asm/volume1-123
Device : /dev/asm/volume1-228
Interface Version: 1
Size (MB): 256
Resize Increment (MB): 32
Redundancy: mirror
Stripe Columns: 4
Stripe Width (KB): 128
Disk Group: DATA
Volume: VOLUME1
Compatible.advm : 11.2.0.0.0

$ /sbin/advmutil volinfo -l /dev/asm/volume1-228
Device : /dev/asm/volume1-228 : Interface Version : 1 : Size (MB) : 256 :
Resize Increment (MB) : 32 : Redundancy : mirror : Stripe Columns : 4 :
Stripe Width (KB) : 128 : Disk Group : DATA : Volume : VOLUME1 :
Compatible.advm : 11.2.0.0.0

$ /sbin/advmutil volinfo -L /dev/asm/volume1-228
/dev/asm/volume1-228 1 256 32 mirror 4 128 DATA VOLUME1 11.2.0.0.0
```

Part IV

Additional Information

Part IV contains the following chapters:

- [Creating Database Files in Oracle ASM Using SQL*Plus](#)
- [Understanding Oracle ACFS Advanced Topics](#)

Creating Database Files in Oracle ASM Using SQL*Plus

This appendix describes how to deploy Oracle Automatic Storage Management (Oracle ASM) using SQL*Plus under the following topics:

- [Creating a Database that Uses Oracle ASM](#)
- [Creating Tablespaces in Oracle ASM](#)
- [Creating Redo Logs in Oracle ASM](#)
- [Creating Control Files in Oracle ASM](#)
- [Creating Archive Log Files in Oracle ASM](#)

See Also:

Oracle Database Administrator's Guide for information about using Oracle Managed Files (OMF)

Creating a Database that Uses Oracle ASM

The recommended method of creating your database is to use Database Configuration Assistant (DBCA). However, if you create your database manually using the `CREATE DATABASE` statement, then Oracle ASM enables you to create a database and all of its underlying files with a minimum of input.

The following example shows the use of the `CREATE DATABASE` statement, where database files are created and managed automatically by Oracle ASM. This example creates a database with the following Oracle ASM files:

- A `SYSTEM` tablespace data file in disk group `data`.
- A `SYSAUX` tablespace data file in disk group `data`. The tablespace is locally managed with automatic segment-space management.
- A multiplexed online redo log with two online log groups, one member of each in `data` and `fra` (fast recovery area).
- If automatic undo management mode is enabled, then an undo tablespace data file in directory `data`.
- If you do not specify a value for the `CONTROL_FILES` initialization parameter, then two control files, one in `data` and another in `fra` (fast recovery area). The control file in `data` is the primary control file.

The following initialization parameter settings are included in the initialization parameter file:

```
DB_CREATE_FILE_DEST = +data
DB_RECOVERY_FILE_DEST = +fra
DB_RECOVERY_FILE_DEST_SIZE = 10G
```

The following statement can be run at the SQL prompt:

```
SQL> CREATE DATABASE orcl;
```

Creating Tablespaces in Oracle ASM

When Oracle ASM creates a data file for a permanent tablespace (or a temporary file for a temporary tablespace), the data file is set to auto-extensible with an unlimited maximum size and 100 MB default size. You can use the `AUTOEXTEND` clause to override this default extensibility and the `SIZE` clause to override the default size.

Oracle ASM applies attributes to the data file, as specified in the system default template for a data file as shown in the table in [“Managing Disk Group Templates”](#). You can also create and specify your own template.

Files in a tablespace might be in both Oracle ASM files and non-Oracle ASM files due to the tablespace history. RMAN commands enable non-Oracle ASM files to be relocated to an Oracle ASM disk group and enable Oracle ASM files to be relocated as non-Oracle ASM files.

For example, if there is a disk group named `data`, then you can create a tablespace `tblspace` in that disk group with the following SQL statement:

```
SQL> CREATE TABLESPACE tblspace DATAFILE '+data';
```

The following example illustrates the usage of Oracle ASM with defaults. This example enables Oracle ASM to create and manage the tablespace data file for you, using Oracle supplied defaults that are adequate for most situations.

Assume the following initialization parameter setting:

```
DB_CREATE_FILE_DEST = +data
```

The following statement creates the tablespace and its data file:

```
SQL> CREATE TABLESPACE tblspace;
```

Creating Redo Logs in Oracle ASM

Online redo logs can be created in multiple disk groups, either implicitly in an initialization parameter file or explicitly in an `ALTER DATABASE . . . ADD LOGFILE` statement. Each online log should have one log member in multiple disk groups. The file names for log file members are automatically generated. All partially created redo log files, created because of a system error, are automatically deleted.

For example, if there are disk groups named `data1` and `data2`, you can create a log file with a member in each disk group with the following SQL statement:

```
SQL> ALTER DATABASE ADD LOGFILE (+data1,+data2);
```

The following example creates a log file with a member in each of the disk groups `data1` and `data2`. These parameter settings are included in the initialization parameter file:

```
DB_CREATE_ONLINE_LOG_DEST_1 = +data1
DB_CREATE_ONLINE_LOG_DEST_2 = +data2
```


The following statement can be run at the SQL prompt:

```
SQL> ALTER DATABASE ADD LOGFILE;
```

Creating Control Files in Oracle ASM

Control files can be explicitly created in multiple disk groups. The file names for control files are automatically generated.

If you must specify a control file by name, then you can use alias file names to reference Oracle ASM files and use easy to understand names. Using aliases in the specification of a control file during its creation enables you to later refer to the control file with a user-specified name. An alias can also be specified as a control file name in the `CONTROL_FILES` initialization parameter.

When creating a control file, data files and log files that are stored in Oracle ASM disk groups should be given to the `CREATE CONTROLFILE` command using the file reference form of their Oracle ASM file names. However, the use of the `RESETLOGS` option requires the use of a file creation form for the specification of the log files.

- [Creating Control Files in Oracle ASM: Example 1](#)
- [Creating Control Files in Oracle ASM: Example 2](#)

Creating Control Files in Oracle ASM: Example 1

The `CREATE CONTROLFILE` SQL statement in [Example 1](#) is generated by an `ALTER DATABASE BACKUP CONTROLFILE TO TRACE` command for a database with data files and log files created on disk groups `data` and `fra`:

Example 1 *Creating control files in Oracle ASM using NORESETLOGS*

```
CREATE CONTROLFILE REUSE DATABASE "ORCL" NORESETLOGS ARCHIVELOG
  MAXLOGFILES 16
  MAXLOGMEMBERS 3
  MAXDATAFILES 100
  MAXINSTANCES 8
  MAXLOGHISTORY 292
LOGFILE
  GROUP 1 (
    '+DATA/orcl/onlinelog/group_1.261.685366203' ,
    '+FRA/orcl/onlinelog/group_1.257.685366205'
  ) SIZE 50M BLOCKSIZE 512,
  GROUP 2 (
    '+DATA/orcl/onlinelog/group_2.262.685366207' ,
    '+FRA/orcl/onlinelog/group_2.258.685366211'
  ) SIZE 50M BLOCKSIZE 512,
  GROUP 3 (
    '+DATA/orcl/onlinelog/group_3.263.685366213' ,
    '+FRA/orcl/onlinelog/group_3.259.685366215'
  ) SIZE 50M BLOCKSIZE 512
-- STANDBY LOGFILE
DATAFILE
  '+DATA/orcl/datafile/system.256.685366089' ,
  '+DATA/orcl/datafile/sysaux.257.685366089' ,
  '+DATA/orcl/datafile/undotbs1.258.685366091' ,
  '+DATA/orcl/datafile/users.259.685366091'
CHARACTER SET WE8MSWIN1252
;
```

Creating Control Files in Oracle ASM: Example 2

[Example 2](#) is a CREATE CONTROLFILE SQL statement for a database with data files, but uses a RESETLOGS clause, which uses the creation form for log files:

Example 2 Creating control files in Oracle ASM using RESETLOGS

```
CREATE CONTROLFILE REUSE DATABASE "ORCL" RESETLOGS ARCHIVELOG
  MAXLOGFILES 16
  MAXLOGMEMBERS 3
  MAXDATAFILES 100
  MAXINSTANCES 8
  MAXLOGHISTORY 292
LOGFILE
  GROUP 1 (
    '+DATA/orcl/onlinelog/group_1.261.685366203',
    '+FRA/orcl/onlinelog/group_1.257.685366205'
  ) SIZE 50M BLOCKSIZE 512,
  GROUP 2 (
    '+DATA/orcl/onlinelog/group_2.262.685366207',
    '+FRA/orcl/onlinelog/group_2.258.685366211'
  ) SIZE 50M BLOCKSIZE 512,
  GROUP 3 (
    '+DATA/orcl/onlinelog/group_3.263.685366213',
    '+FRA/orcl/onlinelog/group_3.259.685366215'
  ) SIZE 50M BLOCKSIZE 512
-- STANDBY LOGFILE
DATAFILE
  '+DATA/orcl/datafile/system.256.685366089',
  '+DATA/orcl/datafile/sysaux.257.685366089',
  '+DATA/orcl/datafile/undotbs1.258.685366091',
  '+DATA/orcl/datafile/users.259.685366091'
CHARACTER SET WE8MSWIN1252
;
```

Creating Archive Log Files in Oracle ASM

Disk groups can be specified as archive log destinations in the LOG_ARCHIVE_DEST and LOG_ARCHIVE_DEST_n initialization parameters. When destinations are specified in this manner, the archive log file names are created in default subdirectories with unique names. However, all LOG_ARCHIVE_DEST_n parameters must have a unique string. To enter the same disk group more than once, subdirectories must be used. For example, you can set LOG_ARCHIVE_DEST_n as follows:

```
LOG_ARCHIVE_DEST_1 = 'LOCATION=+FRA/orcl/arc_1'
LOG_ARCHIVE_DEST_2 = 'LOCATION=+FRA/orcl/arc_2'
...
```

If LOG_ARCHIVE_DEST is set to a disk group name, LOG_ARCHIVE_FORMAT is ignored. Unique filenames for archived logs are automatically created by Oracle Database under default subdirectories. If LOG_ARCHIVE_DEST is set to a directory in a disk group, LOG_ARCHIVE_FORMAT has its normal semantics for the file alias. The underlying file is still generated in the default directories for the disk group with a system generated name.

You can also set the DB_RECOVERY_FILE_DEST initialization parameter to a disk group destination. In [Example 3](#), archive log files are generated with ARCHIVELOG mode enabled, DB_RECOVERY_FILE_DEST set to the +FRA disk group, and ORCL is the value of the DB_UNIQUE_NAME parameter.

See Also:

Oracle Database Administrator's Guide for information about managing archived redo log files

Example 3 Archived log files in an Oracle ASM disk group

```
SQL> SHOW PARAMETER DB_RECOVERY_FILE_DEST
```

NAME	TYPE	VALUE
db_recovery_file_dest	string	+FRA

```
SQL> SELECT SUBSTR(name,1,64) name FROM V$ARCHIVED_LOG;
```

```
NAME
-----
+FRA/ORCL/ARCHIVELOG/2013_06_24/thread_1_seq_112.260.818960623
+FRA/ORCL/ARCHIVELOG/2013_06_24/thread_1_seq_113.261.818978423
+FRA/ORCL/ARCHIVELOG/2013_06_25/thread_1_seq_114.262.818993031
+FRA/ORCL/ARCHIVELOG/2013_06_25/thread_1_seq_115.263.819032439
+FRA/ORCL/ARCHIVELOG/2013_06_25/thread_1_seq_116.264.819047121
+FRA/ORCL/ARCHIVELOG/2013_06_25/thread_1_seq_117.265.819064815
+FRA/ORCL/ARCHIVELOG/2013_06_26/thread_1_seq_118.266.819079417
...
```

Understanding Oracle ACFS Advanced Topics

This appendix discusses Oracle Automatic Storage Management Cluster File System (Oracle ACFS) advanced topics, including limits, advanced administration, and troubleshooting.

See Also:

Articles available at My Oracle Support (<https://support.oracle.com>) for information about Oracle ACFS and Oracle ADVM.

This appendix contains the following topics:

- [Limits of Oracle ACFS](#)
- [Limits of Oracle ADVM](#)
- [Oracle ACFS Drivers Resource Management](#)
- [Oracle ACFS Registry Resource Management](#)
- [Oracle ACFS File System Resource Management](#)
- [Oracle ACFS and Oracle Restart](#)
- [Oracle ACFS Driver Commands](#)
- [Oracle ACFS Plug-in Generic Application Programming Interface](#)
- [Oracle ACFS Tagging Generic Application Programming Interface](#)
- [Understanding Oracle ACFS I/O Failure Console Messages](#)

For an overview of Oracle ACFS, see [Introducing Oracle ACFS and Oracle ADVM](#) .

Limits of Oracle ACFS

The limits of Oracle ACFS are discussed in this section.

The topics contained in this section are:

- [Oracle ACFS Disk Space Usage](#)
- [Oracle ACFS Error Handling](#)
- [Oracle ACFS and NFS](#)

Note:

Oracle ACFS does not support hard links on directories.

Oracle ACFS Disk Space Usage

Oracle ACFS supports 64 mounted file systems on 32-bit systems, and 256 mounts on 64-bit systems. However, more file systems can be mounted if there is adequate memory.

Oracle ACFS supports 2^{40} (1 trillion) files in a file system. More than 4 billion files have been tested. 32-bit Linux systems are limited to 2^{26} (67 million) files. There is no absolute limit to the number of directories in a file system; the limit is based on hardware resources.

Oracle ACFS supports 1023 snapshots on 64-bit systems. These snapshots can be any combination of read-only and read-write snapshots. To support the creation of 1023 snapshots, the disk group compatibility attribute for ADVN must be set to 12.1.0.2 or higher. Before or after setting COMPATIBLE.ADVN to 12.1.0.2, all existing snapshots must be deleted or the limit remains at 63 snapshots.

Oracle ACFS preallocates large user files to improve performance when writing data. This storage is not returned when the file is closed, but it is returned when the file is deleted. Oracle ACFS also allocates local metadata files as nodes mount the file system for the first time. This can result in a mount failing due to an out of space error, and much of this storage must be contiguous. This storage is approximately 64-128 megabytes per node.

Oracle ACFS also keeps local bitmaps available to reduce contention on the global storage bitmap when searching for free space. This disk space is reported as in use by tools such as the Linux `df` command even though some space may not actually be allocated yet. This local storage pool can be as large as 128 megabytes per node and can allow space allocations to succeed, even though commands, such as `df`, report less space available than what is being allocated.

Oracle ACFS Error Handling

Oracle ASM instance failure or forced shutdown while Oracle ACFS or another file system is using an Oracle ADVN volume results in I/O failures. The volumes must be closed and re-opened to access the volume again. This requires dismounting any file systems that were mounted when the local Oracle ASM instance failed. After the instance is restarted, the corresponding disk group must be mounted with the volume enabled followed by a remount of the file system. See [“Deregistering, Dismounting, and Disabling Volumes and Oracle ACFS File Systems”](#).

If any file systems are currently mounted on Oracle ADVN volume files, the SHUTDOWN ABORT command should not be used to terminate the Oracle ASM instance without first dismounting those file systems. Otherwise, applications encounter I/O errors and Oracle ACFS user data and metadata being written at the time of the termination may not be flushed to storage before the Oracle ASM storage is fenced. If there is not time to permit the file system to dismount, then you should run two `sync (1)` commands to flush cached file system data and metadata to persistent storage before issuing the SHUTDOWN ABORT operation.

Oracle ACFS does not interrupt the operating system environment when a metadata write fails, whether due to Oracle ASM instance failure or storage failure. Instead, Oracle ACFS isolates errors to a specific file system, putting it in an offline error state.

The only operation that succeeds on that node for that file system from that point forward is a dismount operation. Another node recovers any outstanding metadata transactions, assuming it can write the metadata out to the storage. It is possible to remount the file system on the offlined node after the I/O condition is resolved.

It might not be possible for an administrator to dismount a file system while it is in the offline error state if there are processes referencing the file system, such as a directory of the file system being the current working directory for a process. To dismount the file system in this case it would be necessary to identify all processes on that node with references to files and directories on the file system and cause them to exit. The Linux `fuser` or `lsof` commands or Windows `handle` command list information about processes and open files.

If Oracle ACFS detects inconsistent file metadata returned from a read operation, based on checksum or expected type comparisons, Oracle ACFS takes the appropriate action to isolate the affected file system components and generate a notification that `fsck` or `acfschkdsk` should be run as soon as possible. Each time the file system is mounted a notification is generated with a system event logger message until `fsck` or `acfschkdsk` is run.

Oracle ACFS and NFS

When exporting file systems through NFS on Linux, use the `-fsid=num` exports option. This option forces the file system identification portion of the file handle used to communicate with NFS clients to be the specified number instead of a number derived from the major and minor number of the block device on which the file system is mounted. You can use any 32-bit number for `num`, but it must be unique among all the exported file systems. In addition, `num` must be unique among members of the cluster and must be the same `num` on each member of the cluster for a given file system. This is needed because Oracle ASM DVM block device major numbers are not guaranteed to be the same across restarts of the same node or across different nodes in the cluster.

When using High Availability NFS for Grid Home Clusters (HANFS), HANFS automatically handles the situation described in the previous paragraph. For information about HANFS, refer to [“High Availability Network File Storage for Oracle Grid Infrastructure”](#).

Limits of Oracle ADVM

The limits of Oracle ADVM and these discussed in this section.

The default configuration for an Oracle ADVM volume is 8 columns and a 1 MB stripe width. The volume extent size is 8 megabytes (MB) if the disk group allocation unit (AU) is less than or equal to 8 MB. If the AU size is greater than 8 MB, then the Oracle ADVM volume extent size is equivalent to the disk group AU size.

Oracle ADVM writes data as 1 megabyte (MB) stripe chunks in round robin fashion to each column and fills a stripe set of eight 8 MB extents with 64 stripe chunks before moving to a second stripe set of eight 8 MB extents for volumes greater than 64 MB. Setting the number of columns on an Oracle ADVM dynamic volume to 1 effectively turns off striping for the Oracle ADVM volume.

On Linux platforms Oracle ASM Dynamic Volume Manager (Oracle ADVM) volume devices are created as block devices regardless of the configuration of the underlying storage in the Oracle ASM disk group. Do not use `raw (8)` to map Oracle ADVM volume block devices into raw volume devices.

For information about ASMCMD commands to manage Oracle ADVM volumes, refer to [Managing Oracle ADVM with ASMCMD](#).

Oracle ACFS Drivers Resource Management

Oracle ACFS, Oracle ADVM, and OKS drivers are loaded during the start of the Oracle Grid Infrastructure stack, except in an Oracle Restart configuration. The drivers remain loaded until the system is rebooted, at which point, they are loaded again when the Oracle Grid Infrastructure stack restarts.

For information about commands to manage Oracle ACFS, Oracle ADVM, and OKS drivers, refer to [“Oracle ACFS Driver Commands”](#).

Oracle ACFS Registry Resource Management

The Oracle ACFS registry resource is supported only for Oracle Grid Infrastructure cluster configurations; it is not supported for Oracle Restart configurations. See [“Oracle ACFS and Oracle Restart”](#).

With Oracle ASM 12c Release 1 (12.1), the Oracle ACFS registry uses the standard single file system resource available through the SRVCTL file system interface. For more information, refer to [“Oracle ACFS File System Resource Management”](#). Using SRVCTL enables applications to depend on registered file systems, such as for management of the registered file systems using `srvctl filesystem`. By default, `acfsutil registry` shows only file systems that are set to be always mounted, with the `AUTO_START` attribute set to `always`.

The Oracle ACFS registry requires root privileges to register and delete file systems, however, other users can be entitled to start and stop (mount and unmount) the file systems by use of the `user` option.

Oracle ACFS File System Resource Management

The Oracle ACFS file system resource is supported only for Oracle Grid Infrastructure cluster configurations; it is not supported for Oracle Restart configurations. See [“Oracle ACFS and Oracle Restart”](#).

Oracle ASM Configuration Assistant (ASMCA) facilitates the creation of Oracle ACFS file system resources (`ora.diskgroup.volume.acfs`). During database creation with Database Configuration Assistant (DBCA), the Oracle ACFS file system resource is included in the dependency list of its associated disk group so that stopping the disk group also attempts to stop any dependent Oracle ACFS file systems.

An Oracle ACFS file system resource is typically created for use with application resource dependency lists. For example, if an Oracle ACFS file system is configured for use as an Oracle Database home, then a resource created for the file system can be included in the resource dependency list of the Oracle Database application. This dependency causes the file system and stack to be automatically mounted due to the start action of the database application.

The start action for an Oracle ACFS file system resource is to mount the file system. This Oracle ACFS file system resource action includes confirming that the associated file system storage stack is active and mounting the disk group, enabling the volume file, and creating the mount point if necessary to complete the mount operation. If the file system is successfully mounted, the state of the resource is set to `online`; otherwise, it is set to `offline`.

The check action for an Oracle ACFS file system resource verifies that the file system is mounted. It sets the state of the resource to `online` status if mounted, otherwise the status is set to `offline`.

The stop action for an Oracle ACFS file system resource attempts to dismount the file system. If the file system cannot be dismounted due to open references, the stop action displays and logs the process identifiers for any processes holding a reference.

Use of the `srvctl start` and `stop` actions to manage the Oracle ACFS file system resources maintains their correct resource state.

Oracle ACFS and Oracle Restart

Oracle Restart does not support root-based Oracle ACFS resources for this release. Consequently, the following operations are not automatically performed:

- Loading Oracle ACFS drivers
You can load or unload the drivers manually with the `acfsload` command. For more information, refer to [“acfsload”](#).
- Mounting Oracle ACFS file systems listed in the Oracle ACFS mount registry
You can mount Oracle ACFS file systems manually with the `mount` command. For information, refer to [Managing Oracle ACFS with Command-Line Tools](#).
- Mounting resource-based Oracle ACFS database home file systems

The Oracle ACFS resources associated with these actions are not created for Oracle Restart configurations.

While Oracle ACFS resource management is fully supported for Oracle Grid Infrastructure configurations, the Oracle ACFS resource-based management actions must be replaced with alternative, sometimes manual, operations in Oracle Restart configurations.

Oracle ACFS Driver Commands

This section describes the Oracle ACFS driver commands that are used during installation to manage Oracle ACFS, Oracle ADVM, and Oracle Kernel Services Driver (OKS) drivers. These commands are located in the `/bin` directory of the Oracle Grid Infrastructure home.

- [acfsload](#)
- [acfsdriverstate](#)

acfsload

Purpose

`acfsload` loads or unloads Oracle ACFS, Oracle ADVM, and Oracle Kernel Services Driver (OKS) drivers.

Syntax

```
acfsload { start | stop } [ -s ]
```

[Table 1](#) contains the options available with the `acfsload` command.

Table 1 Options for the `acfsload` command

Option	Description
<code>start</code>	Loads the Oracle ACFS, Oracle ADVM, and OKS drivers.
<code>stop</code>	Unloads the Oracle ACFS, Oracle ADVM, and OKS drivers.
<code>-s</code>	Operate in silent mode.

Description

You can use `acfsload` to manually load or unload the Oracle ACFS, Oracle ADVM, and OKS drivers.

Before unloading drivers with the `stop` option, you must dismount Oracle ACFS file systems and shut down Oracle ASM. For information about dismounting Oracle ACFS file systems, refer to [“Deregistering_ Dismounting_ and Disabling Volumes and Oracle ACFS File Systems”](#).

`root` or administrator privilege is required to run `acfsload`.

Examples

The following is an example of the use of `acfsload` to stop (unload) all drivers.

```
# acfsload stop
```

acfsdriverstate**Purpose**

`acfsdriverstate` provides information on the current state of the Oracle ACFS, Oracle ADVM, and Oracle Kernel Services Driver (OKS) drivers.

Syntax

```
acfsdriverstate [-orahome ORACLE_HOME ]
                { installed | loaded | version | supported }
```

[Table 2](#) contains the options available with the `acfsdriverstate` command.

Table 2 Options for the `acfsdriverstate` command

Option	Description
<code>-orahome ORACLE_HOME</code>	Specifies the Oracle Grid Infrastructure home in which the user has permission to execute the <code>acfsdriverstate</code> command.
<code>installed</code>	Determines whether Oracle ACFS is installed on the system.
<code>loaded</code>	Determines whether the Oracle ADVM, Oracle ACFS, and OKS drivers are loaded in memory.
<code>version</code>	Reports the currently installed version of the Oracle ACFS system software.
<code>supported</code>	Reports whether the system is a supported kernel for Oracle ACFS.

Description

You can use `acfsdriverstate` to display detailed information on the current state of the Oracle ACFS, Oracle ADVM, and OKS drivers.

Examples

The following is an example of the use of `acfsdriverstate`.

```
$ acfsdriverstate -orahome /users/12.1.0/grid/ version
ACFS-9325:      Driver OS kernel version = 2.6.18-8.el5xen(x86_64)
ACFS-9326:      Driver Oracle version = 120209
```

Oracle ACFS Plug-in Generic Application Programming Interface

Oracle ACFS plug-in operations are supported through a common, operating system (OS) independent file plug-in (C library) application programming interface (API).

The topics contained in this section are:

- [Oracle ACFS Pre-defined Metric Types](#)
- [acfsplugin](#)

For more information about Oracle ACFS plug-ins, refer to “[Oracle ACFS Plugins](#)”.

Oracle ACFS Pre-defined Metric Types

Oracle ACFS provides the `acfsmetric1` pre-defined metric type.

The `acfsmetric1` metric set is defined for the storage virtualization model. The metrics are maintained as a summary record for either a selected set of tagged files or all files in the file system. Oracle ACFS file metrics include: number of reads, number of writes, average read size, average write size, minimum and maximum read size, minimum and maximum write size, and read cache (VM page cache) hits and misses.

Example:

```
typedef struct _ACFS_METRIC1 {
    ub2 acfs_version;
    ub2 acfs_type;
    ub4 acfs_seqno;
    ub8 acfs_nreads;
    ub8 acfs_nwrites;
    ub8 acfs_rcachehits;
    ub4 acfs_avgrsize;
    ub4 acfs_avgwsize;
    ub4 acfs_minrsize;
    ub4 acfs_maxrsize;
    ub4 acfs_minwsize;
    ub4 acfs_maxwsize;
    ub4 acfs_rbytes_per_sec;
    ub4 acfs_wbytes_per_sec;
    ub8 acfs_timestamp;
    ub8 acfs_elapsed_secs;
} ACFS_METRIC1;
```

acfsplugin

Purpose

The `acfsplugin` application programming interface (API) sends and receives messages to and from the local plug-in enabled Oracle ACFS driver from the application plug-in module.

Syntax

```
sb8 acfsplugin_metrics(ub4 metric_type,
    ub1 *metrics,
```

```
ub4 metric_buf_len,  
oratest *mountp );
```

Description

The Oracle ACFS plug-in API is used by an Oracle ACFS application plug-in module to retrieve metrics from the Oracle ACFS driver. The Oracle ACFS driver must first be enabled for plug-in communication using the `acfsutil plugin enable` command. The selected application plug-in metric type model must match the plug-in configuration defined with the Oracle ACFS plug-in enable command. For information about the `acfsutil plugin enable` command, refer to “[acfsutil plugin enable](#)”. The application must provide a buffer large enough to store the metric structures described in “[Oracle ACFS Pre-defined Metric Types](#)”.

If the provided buffer is `NULL` and `metric_buf_len = 0`, the return value is the size required to hold all the currently collected metrics. The application can first query Oracle ACFS to see how big a buffer is required, then allocate a buffer of the necessary size to pass back to Oracle ACFS.

The mount path must be provided to the API to identify the plug-in enabled Oracle ACFS file system that is being referenced.

A nonnegative value is returned for success: 0 for success with no more metrics to collect, 1 to indicate that more metrics are available, or 2 to indicate that no new metrics were collected during the interval. In the case of an error, a negative value is returned and `errno` is set on Linux environments or `SetLastError` is called on Windows.

System administrator or Oracle ASM administrator privileges are required to send and receive messages to and from the plug-in enabled Oracle ACFS file system driver.

Writing Applications

To use the plugin API, applications must include the C header file `acfslib.h` which defines the API functions and structures.

```
#include <acfslib.h>
```

When building the application executable, the application must be linked with the `acfs12` library. Check the platform-specific documentation for information about environment variables that must be defined. For example:

```
export LD_LIBRARY_PATH=${ORACLE_HOME}/lib:${  
{LD_LIBRARY_PATH}}
```

Then when linking, add the `-lacfs12` flag.

Examples

In [Example 1](#), the command enables an Oracle ACFS file system mounted on `/humanresources` for the plug-in service.

Example 1 Application Plug-in for Storage Visibility: Poll Model

```
$ /sbin/acfsutil plugin enable -m acfsmetric1 -t HRDATA /humanresources
```

With this command, the application plug-in polls the Oracle ACFS plug-in enabled driver for summary metrics associated with files tagged with `HRDATA`. The application code includes the following:

```
#include <acfslib.h>  
...
```

```

/* allocate message buffers */
ACFS_METRIC1 *metrics = malloc (sizeof(ACFS_METRIC1));
/* poll for metric1 data */
while (condition) {
    /* read next summary message from ACFS driver */
    if ((rc = acfsplugin_metrics(ACFS_METRIC_TYPE1,
(ubl*)metrics,sizeof(*metrics),
    mountp)) < 0) {
        perror("...Receive failure ... ");
        break;
    }
    /* print message data */
    printf ("reads %8llu ", metrics->acfs_nreads);
    printf("writes %8llu ", metrics->acfs_nwrites);
    printf("avg read size %8u ", metrics->acfs_avgrsize);
    printf("avg write size %8u ", metrics->acfs_avgwsize);
    printf("min read size %8u ", metrics->acfs_minrsize);
    printf("max read size %8u ", metrics->acfs_maxrsize);
    ...
    sleep (timebeforenextpoll);
}

```

In [Example 2](#), the command enables an Oracle ACFS file system mounted on /humanresources for the plug-in service.

Example 2 Application Plug-in for File Content: Post Model

```
$ /sbin/acfsutil plugin enable -m acfsmetric1 -t HRDATA -i 5m /humanresources
```

With this command, every 5 minutes the Oracle ACFS plug-in enabled driver posts file content metrics associated with files tagged with HRDATA. In the application code, the call to `acfsplugin_metrics()` is blocked until the metrics are posted. The application code includes the following:

```

#include <acfslib.h>
...
ACFS_METRIC1 *metrics = malloc (sizeof(ACFS_METRIC1));

/* Wait for metric Data */
while (condition) {
    /* Wait for next file content posting from ACFS driver */
    rc = ACFS_PLUGIN_MORE_AVAIL;
    /* A return code of 1 indicates that more metrics are available
    * in the current set of metrics.
    */
    while( rc == ACFS_PLUGIN_MORE_AVAIL) {
        /* This call blocks until metrics are available. */
        rc = acfsplugin_metrics(ACFS_METRIC_TYPE1, (ubl*)metrics, sizeof(*metrics),
            mountp);
        if (rc < 0) {
            perror("...Receive failure ... ");
            break;
        } else if (rc == ACFS_PLUGIN_NO_NEW_METRICS) {
            printf("No new metrics available.");
            break;
        }
    }
    if (last_seqno != metrics->acfs_seqno-1) {
        printf("Warning: Unable to keep up with metrics collection.");
        printf("Missed %d sets of posted metrics.",
            (metrics->acfs_seqno-1)-last_seqno);
    }

    /* print message data */
    printf ("reads %8llu ", metrics->acfs_nreads);
    printf("writes %8llu ", metrics->acfs_nwrites);
    printf("avg read size %8u ", metrics->acfs_avgrsize);
    printf("avg write size %8u ", metrics->acfs_avgwsize);

```

```
printf("min read size %8u ", metrics->acfs_minrsize);
printf("max read size %8u ", metrics->acfs_maxrsize);
...

    last_seqno = metrics->acfs_seqno;
}
}

free(metrics);
```

Oracle ACFS Tagging Generic Application Programming Interface

Oracle ACFS tagging operations are supported through a common operating system (OS) independent file tag (C library) application programming interface (API).

An Oracle ACFS tagging API demonstration utility is provided. The demo provides instructions to build the utility with a makefile on each supported platform.

On Solaris, Oracle ACFS tagging APIs can set tag names on symbolic link files, but backup and restore utilities do not save the tag names that are explicitly set on the symbolic link files. Also, symbolic link files lose explicitly set tag names if they have been moved, copied, tarred, or paxed.

The following files are included:

- `$ORACLE_HOME/usm/public/acfslib.h`
- `$ORACLE_HOME/usm/demo/acfstagsdemo.c`
- `$ORACLE_HOME/usm/demo/Makefile`

Linux, Solaris, or AIX makefile for creating the demo utility.

- `$ORACLE_HOME/usm/demo/MAKEFILE`

Windows demo utility MAKEFILE (for use by the nmake utility) to create the demo utility.

The topics contained in this section are:

- [Oracle ACFS Tag Name Specifications](#)
- [Oracle ACFS Tagging Error Values](#)
- [acfsgettag](#)
- [acfslisttags](#)
- [acfsremovetag](#)
- [acfssettag](#)

Oracle ACFS Tag Name Specifications

An Oracle ACFS tag name can be from 1 to 32 characters in length and consist of a combination of the following set of characters only:

- uppercase and lowercase alphabetic characters (A-Z, a-z)
- numbers (0-9)
- hyphen (-)

- underscore (_)
- blank (space)

Oracle ACFS Tagging Error Values

The following are the values for Linux, Solaris, or AIX `errno` in case of failure:

- `EINVAL` – The tag name syntax is invalid or too long.
- `ENODATA` – The tag name does not exist for this file or directory.
- `ERANGE` - The value buffer is too small to hold the returned value.
- `EACCES` – Search permission denied for a directory in the path prefix of path; or the user does not have permission on the file to read tag names.
- `ENAMETOOLONG` – The file name is too long.
- `ENOENT` – A component of path does not exist.

The following are the values that Windows `GetLastError()` returns in case of failure:

- `ERROR_INVALID_PARAMETER` - The tag name does not exist for this file or directory or the tag name is syntactically incorrect.
- `ERROR_INSUFFICIENT_BUFFER` - The value buffer is too small to hold the returned value.
- `ERROR_ACCESS_DENIED` - Search permission denied for a directory in the path prefix of path; or the user does not have permission on the file to read tag names.
- `ERROR_INVALID_NAME` - The file name or path name is too long or is malformed.
- `ERROR_FILE_NOT_FOUND` - The system cannot find the file specified.

acfsgettag

Purpose

Retrieves the value associated with an Oracle ACFS file tag name.

Syntax

```
sb8 acfsgettag(const oratext *path, const oratext *tagname, oratext *value,
              size_t size, ub4 flags);
```

[Table 3](#) contains the options available with the `acfsgettag` command.

Table 3 Options for the `acfsgettag` command

Option	Description
<i>path</i>	Specifies a pointer to a file or directory path name.
<i>tagname</i>	Specifies a pointer to a NULL-terminated Oracle ACFS tag name in the format of a valid tag name for regular files and directories.

Option	Description
<i>value</i>	Specifies the memory buffer to retrieve the Oracle ACFS tag value.
<i>size</i>	Specifies the byte size of the memory buffer that holds the returned Oracle ACFS tag value.
<i>flags</i>	Reserved for future use. Must be set to 0.

Description

The `acfsgettag` library call retrieves the value string of the Oracle ACFS tag name. The return value is the nonzero byte length of the output *value* string on success or `ACFS_TAG_FAIL` on failure. For information about operating system-specific extended error information values that may be obtained when an `ACFS_TAG_FAIL` is returned, refer to [“Oracle ACFS Tagging Error Values”](#).

Because Oracle ACFS tag names currently use a fixed value string of 0 (the number zero character with a byte length of one) the value is the same for all Oracle ACFS tag name entries. The size of the *value* buffer can be determined by calling `acfsgettag` with a NULL *value* and 0 *size*. The library call returns the byte size necessary to hold the value string of the tag name. `acfsgettag` returns an `ENODATA` error when the tag name is not set on the file.

Examples

[Example 3](#) is an example of the use of the `acfsgettag` function call.

Example 3 Retrieving a file tag value

```

sb8 rc;
size_t size;
oratext value[2];
const oratext *path = "/mnt/dir1/dir2/file2";
const oratext *tagname = "patch_set_11_1";
size = 1; (byte)
memset((void *)value, 0, 2*sizeof(oratext));
rc = acfsgettag (path, tagname, value, size, 0);
If (rc == ACFS_TAG_FAIL)
    /* check errno or GetLastError() to process error returns */

```

acfslisttags

Purpose

Lists the tag names assigned to an Oracle ACFS file. For additional information, refer to [“acfsutil tag info”](#).

Syntax

```
sb8 acfslisttags(const oratext *path, oratext *list, size_t size, ub4 flags);
```

[Table 3](#) contains the options available with the `acfslisttags` command.

Table 4 Options for the `acfslisttags` command

Option	Description
<i>path</i>	Specifies a pointer to a file or directory path name.

Option	Description
<i>list</i>	Specifies a pointer to a memory buffer containing the list of Oracle ACFS tag names.
<i>size</i>	Specifies the size (bytes) of the memory buffer that holds the returned Oracle ACFS tag name list.
<i>flags</i>	Reserved for future use. Must be set to 0.

Description

The `acfslisttags` library call retrieves all the tag names assigned to an Oracle ACFS file. `acfslisttags` returns a list of tag names into the `list` memory buffer. Each tag name in the list is terminated with a NULL. If a file has no tag names then the list is empty. The memory buffer must be large enough to hold all of the tag names assigned to an Oracle ACFS file.

An application must allocate a buffer and specify a list size large enough to hold all of the tag names assigned to an Oracle ACFS file. An application can optionally obtain the list buffer size needed by first calling `acfslisttags` with a zero value buffer size and NULL list buffer. The application then checks for nonzero, positive list size return values to allocate a list buffer and call `acfslisttags` to retrieve the actual tag name list.

On success, the return value is a positive byte size of the tag name list or 0 when the file has no tag names. On failure, the return value is `ACFS_TAG_FAIL`. For information about operating system-specific extended error information values that may be obtained when an `ACFS_TAG_FAIL` is returned, refer to [“Oracle ACFS Tagging Error Values”](#).

Examples

[Example 4](#) is an example of the use of the `acfslisttags` function call.

Example 4 Listing file tags

```

sb8 listsize;
sb8 listsize2;
const oratext *path = "/mnt/dir1/dir2/file2";
oratext *list;
/* Determine size of buffer to store list */
listsize = acfslisttags (path, NULL, 0, 0);
if (listsize == ACFS_TAG_FAIL)
/* retrieve the error code and return */

if (listsize)
{
    list = malloc(listsize)
    /* Retrieve list of tag names */
    listsize2 = acfslisttags (path, list, listsize, 0);
    if (listsize2 == ACFS_TAG_FAIL)
        /* check errno or GetLastError() to process error returns */
    if (listsize2 > 0)
        /* file has a list of tag names to process */
    else
        /* file has no tag names. */
}
else
/* file has no tag names. */

```

acfsremovetag

Purpose

Removes the tag name on an Oracle ACFS file.

Syntax

```
sb8 acfsremovetag(const oratext *path, const oratext *tagname, ub4 flags);
```

[Table 5](#) contains the options available with the `acfsremovetag` command.

Table 5 Options for the `acfsremovetag` command

Option	Description
<i>path</i>	Specifies a pointer to a file or directory path name.
<i>tagname</i>	Specifies a pointer to a NULL-terminated Oracle ACFS tag name in the format of a valid tag name for regular files and directories.
<i>flags</i>	Reserved for future use. Must be set to 0.

Description

The `acfsremovetag` library call removes a tag name on an Oracle ACFS file. The return value is `ACFS_TAG_SUCCESS` or `ACFS_TAG_FAIL`. For information about operating system-specific extended error information values that may be obtained when an `ACFS_TAG_FAIL` is returned, refer to [“Oracle ACFS Tagging Error Values”](#).

Examples

[Example 5](#) is an example of the use of the `acfsremovetag` function call.

Example 5 Removing file tags

```
sb8 rc;
const oratext *path= "/mnt/dir1/dir2/file2";
const oratext *tagname = "patch_set_11_1";
rc = acfsremovetag (path, tagname, 0);
If (rc == ACFS_TAG_FAIL)
    /* check errno or GetLastError() to process error returns */
```

acfssettag

Purpose

Sets the tag name on an Oracle ACFS file. For additional information, refer to [“acfsutil tag set”](#).

Syntax

```
sb8 acfssettag(const oratext *path, const oratext *tagname, oratext *value,
               size_t size, ub4 flags);
```

[Table 6](#) contains the options available with the `acfssettag` command.

Table 6 Options for the acfssettag command

Option	Description
<i>path</i>	Specifies a pointer to a file or directory path name.
<i>tagname</i>	Specifies a pointer to a NULL-terminated Oracle ACFS tag name in the format of a valid tag name for regular files and directories.
<i>value</i>	Specifies the memory buffer to set the Oracle ACFS tag value.
<i>size</i>	Specifies the byte size of the Oracle ACFS tag value.
<i>flags</i>	Reserved for future use. Must be set to 0.

Description

The `acfssettag` library call sets a tag name on an Oracle ACFS file. The return value is `ACFS_TAG_SUCCESS` or `ACFS_TAG_FAIL`. For information about operating system-specific extended error information values that may be obtained when an `ACFS_TAG_FAIL` is returned, refer to “[Oracle ACFS Tagging Error Values](#)”.

Because Oracle ACFS tag names currently use a fixed value string of 0 (the number zero character with a byte length of one) the *value* is the same for all Oracle ACFS tag name entries.

Examples

[Example 6](#) is an example of the use of the `acfssettag` function call.

Example 6 Setting file tags

```
sb8 rc;
size_t size;
const oratext *value ;
const oratext *path= "/mnt/dir1/dir2/file2";
const oratext *tagname = "patch_set_11_1";
value = "0"; /* zero */
size = 1; (byte)
rc = acfssettag (path, tagname, (oratext *)value, size, 0);
If (rc == ACFS_TAG_FAIL)
    /* check errno and GetLastError() to process error returns */
```

Understanding Oracle ACFS I/O Failure Console Messages

Oracle ACFS logs information for I/O failures in the operating-specific system event log.

A console message has the following format:

```
[Oracle ACFS]: I/O failure (error_code) with device device_name during a operation_name op_type.
file_entry_num Starting offset: offset. Length of data transfer: io_length bytes.
Impact: acfs_type Object: object_type Oper.Context: operation_context
Snapshot?: yes_or_no AcfsObjectID: acfs_object_id . Internal ACFS Location: code_location.
```

The italicized variables in the console message syntax correspond to the following:

- I/O failure

The operating system-specific error code, in Hex, seen by Oracle ACFS for a failed I/O. This may indicate a hardware problem, or it might indicate a failure to initiate the I/O for some other reason.

- Device
The device involved, usually the ADVN device file, but under some circumstances it might be a string indicating the device minor number
- Operation name
The kind of operation involved:
user data, metadata, or paging
- Operation type
The type of operation involved:
synch read, synch write, asynch read, or asynch write
- File entry number
The Oracle ACFS File entry number of the file system object involved, as a decimal number. The `acfsutil info fileid` tool finds the corresponding file name.
- Offset
The disk offset of the I/O, as a decimal number.
- Length of I/O
The length of the I/O in bytes, as decimal number.
- File system object impacted
An indication that the file system object involved is either node-local, or is a resource accessed clusterwide. For example:
Node or Cluster
- Type of object impacted
A string indicating the kind of file system object involved, when possible. For example:
Unknown, User Dir ., User Symlink, User File, Sys.Dir, Sys.File, or MetaData
 - Sys.Dir.
Oracle ACFS-administered directory within the visible namespace
 - sys.File
Oracle ACFS-administered file within the visible namespace
 - MetaData
Oracle ACFS-administered resources outside of the visible namespace
- Operational context
A higher-level view of what code context was issuing the I/O. This is for use by Oracle Support Services. For example:
Unknown, Read, Write, Grow, Shrink, Commit, or Recovery
- Snapshot

An indication of whether, if possible to determine, the data involved was from a Snapshot. For example:

Yes, No, or ?

- Object type of the file system

An internal identifier for the type of file system object. For use by Oracle Support Services.

- Location of the code

An internal identifier of the code location issuing this message. For use by Oracle Support Services.

The following is an example from `/var/log/messages` in a Linux environment:

```
[Oracle ACFS]: I/O failure (0xc0000001) with device /dev/sdb during a metadata synch write .  
Fenum Unknown. Starting offset: 67113984. Length of data transfer: 2560 bytes.  
Impact: Node   Object: MetaData   Oper.Context: Write  
Snapshot?: ?  AcfsObjectID: 8   . Internal ACFS Location: 5 .
```


ASMLIB

ASMLIB is an application programming interface (API) developed by Oracle to simplify the operating system-to-database interface and to exploit the capabilities of vendors' storage arrays on Linux-based systems.

Oracle ASM Filter Driver is the recommended replacement for ASMLIB. For information about Oracle ASM Filter Driver, refer to "[Oracle ASM Filter Driver](#)".

Cluster File System (CFS)

A Cluster File System, or CFS, is a file system that is distributed across multiple computer systems. Generally, the computer systems share access to a disk connected through a [Storage Area Network \(SAN\)](#). The CFS component on each individual computer system coordinates access to the disks using a global communication mechanism.

Cluster Synchronization Services (CSS)

Cluster Synchronization Services (CSS) provide the foundation for coordinated, inter-process communication activities across a set of nodes. CSS services include group services, lock services, node information and cluster configuration services, and node monitoring services that detect nodes joining and leaving the cluster.

CSS Cluster

A CSS cluster is the cluster configuration defined by the CSS cluster membership services. CSS maintains the authoritative membership for an Oracle cluster and monitors nodes joining and leaving the cluster configuration. There is at most one CSS cluster defined for a given set of nodes.

disk group

An Oracle ASM disk group is a collection of disks that Oracle ASM manages as a unit. Within a disk group, Oracle ASM exposes a file system interface for Oracle Database files. The content of files that are stored in a disk group are evenly distributed, or striped, to eliminate hot spots and to provide uniform performance across the disks. Oracle ASM files may also be optionally mirrored within a disk group. The performance of disks in a disk group is comparable to the performance of raw devices.

Direct Attached Storage (DAS)

Direct Attached Storage, or DAS, consists of storage devices that attach directly to host without an intervening network. DAS generally costs less than SAN attached storage, but also offers less flexibility and functionality. Examples of DAS include SATA disks, common to most desktop systems, and SCSI disks that are found on many servers.

extent

An extent, also called data extent, is the raw storage used to hold the contents of a file. Each extent consists of one or more allocation units (AU) on a specific disk.

extent map

An extent map is a list of extent pointers that point to all the data extents of a file. This is the raw storage for the file. Each extent pointer gives the disk and allocation unit of the data extent. For reliability, each extent pointer also includes a check byte to ensure it has not been damaged. This is particularly important when using an in-memory copy of the extent map to direct file I/O to a particular disk location.

fibre channel

Fibre channel is a set of standards that define the interface between computer systems and peripherals. The fibre channel interface is a serial bus interface originally designed to supersede the SCSI standard. However, both the fibre channel and SCSI interfaces have evolved independently of each other and have benefited from the existence of the other. Fibre is spelled with **re** rather than an **er** to indicate a distinction from terms such as *fiber optics*. Both copper and optical fiber are commonly used as a media for fibre channel.

file system

A file system is a software component providing structured access to disks. File systems present objects, such as files, to application programs. Access to files is generally specified with standard API defining operating system calls such as Open/Close and Read/Write that the application program uses for accessing files. File systems are usually provided as a component of an operating system, but may be provided as an independent software component.

file

A file is an object presented to an application program by a [file system](#). A file is subdivided into blocks by the file system. A file system typically places what appears to the application program as consecutive blocks, into nonconsecutive locations on disks. The mapping of the file blocks to the locations on disks is kept in what is known as an [extent map](#).

host bus adapter (HBA)

A host bus adapter (HBA), or host adapter, connects a host system to other network and storage devices, such as, eSATA, and SCSI devices.

Logical Unit Number (LUN)

In storage technology, the term LUN is often used to denote a disk presented to a computer system by a storage array. In SCSI terminology, a Logical Unit Number, or LUN, is a number representing a device address presented to a computer system.

mirroring

In storage systems, mirroring is a means for protecting the integrity of data by storing copies of data on multiple disks. If a disk fails, then a secondary copy of the data is available on a second or third disk. Generally, mirroring can be deployed in one of two ways. In the most common case, as with a RAID storage array, a fixed amount of physical storage space on a single disk is uniformly copied on multiple disks. Through software on the storage array, the physically mirrored space on multiple devices is presented to the host as a single disk. Another approach to mirroring is to copy fixed segments of a file onto multiple disks. Oracle ASM uses the second approach for maximum flexibility.

Network Attached Storage (NAS)

Network Attached Storage, or NAS, comprises a class of systems providing file services to host computers. A device driver in the operating system accesses data using protocols such as NFS or Common Internet File System (CIFS). From the application program's point of view, Network Attached Storage appears as a file system local to the host computer on which the application program resides.

Network File System (NFS)

A network file system, or NFS, is an industry standard providing Network Attached Storage on many platforms. NFS extends the local file system framework to provide device sharing to users on an IP network. The user view of an NFS is that a remote file system on a host appears as if it were locally mounted.

Oracle Automatic Storage Management Cluster

An Oracle Automatic Storage Management (Oracle ASM) cluster is a collection of interconnected nodes, each with an Oracle ASM instance, operating as a unified cluster using Oracle Clusterware. An Oracle ASM cluster presents a shared pool of storage to one or more Oracle Databases that are also operating on the nodes. The databases can also be clustered using Oracle Real Application Clusters, but that is not a requirement. The disks that provide the shared storage pool must be accessible from all of the nodes in the Oracle ASM cluster.

partition

Operating systems typically provide a means for splitting a disk into sections called partitions. To an application, a partition appears as an independent disk, even though that is not the case. The operating system provides a command for managing the size and locations of partitions on a disk. This command writes a partition map onto the disk in an area that is not visible to the application program.

Redundant Array of Inexpensive Disks (RAID)

Redundant Array of Inexpensive Disks, or RAID, is a means for combining multiple disks through software and presenting them to a host as a collection of apparently distinct disks. Mirroring and striping are two means used for combining the disks as a collection. RAID can be implemented as a software component of a computer system or as software operating inside of a storage array. RAID operates on the physical

presentation of storage as opposed to Oracle ASM mirroring and striping at the logical file level.

Storage Area Network (SAN)

Storage Area Network, or SAN, is a specialized network designed for attaching storage devices, such as disk arrays and tape drives, to computer systems. The most common network infrastructure used in SANs is [fibre channel](#). SANs provide great flexibility by allowing a common interconnect infrastructure in which any storage device can be connected to any computer system. Zoning and LUN masking are commonly used for access control for SANs. Zoning is a mechanism where the SAN infrastructure determines the access rights of storage devices to computer systems. LUN masking is a mechanism where the storage device determines the access rights of what computer systems are permitted to connect to the device.

Small Computer System Interface (SCSI)

Small Computer System Interface, or SCSI, is a standard defining the interface between computer systems and peripherals, most commonly storage devices. The SCSI standard defines both the logical and physical aspects of the interface between computer systems and peripherals.

striping

In storage systems, striping is a means for spreading data across multiple disks as opposed to storing the data on a single disk. Striping is usually done to improve performance. Generally, striping can be deployed in one of two ways. In the most common case, as with a RAID storage array, a fixed amount of physical storage space that could have been stored on a single disk is uniformly striped across multiple disks. Through software on the storage array, the physically striped space on multiple devices is presented to the host as a single disk. Another approach to striping is to stripe fixed segments of a file across multiple disks connected to the host. Oracle ASM uses the second approach for maximum performance.

volume

In the storage realm, the meaning of volume has many related definitions. Volumes are often thought of as the virtual entity represented as a [Logical Unit Number \(LUN\)](#). Volumes often are presented as an aggregation of pieces from several disks. A volume is managed by a software component called a [volume manager](#).

volume manager

A volume manager is a software component that manages the mapping of the collection of the pieces of the disks into a [volume](#).

Symbols

.ACFS directory
Oracle ACFS snapshots, [11-10](#), [16-125](#)

A

accelerator volume
enabled by compatibility attributes, [4-47](#)
Oracle ADVM, [4-47](#), [16-25](#)

access control
disk groups, [4-49](#)

ACCESS_CONTROL.ENABLED disk group attribute, [4-3](#), [4-51](#)

ACCESS_CONTROL.UMASK disk group attribute, [4-3](#), [4-51](#)

ACFS *See* Oracle Automatic Storage Management Cluster File System

acfschkdsk command, [16-41](#)

acfsdbg command, [16-108](#)

acfsdismount command, [16-43](#)

acfsdriverstate
Oracle ACFS driver command, [18-6](#)

acfsformat command, [16-44](#)

acfsgettag
Oracle ACFS tagging API, [18-11](#)

acfslisttags
Oracle ACFS tagging API, [18-12](#)

acfsload
Oracle ACFS driver command, [18-5](#)

AcfsMaxCachedFiles
Oracle ACFS tunable parameter, [16-129](#)

AcfsMaxOpenFiles
Oracle ACFS tunable parameter, [16-129](#)

acfsmountvol command, [16-45](#)

acfsplugin
Oracle ACFS API, [18-7](#)

acfsremovetag
Oracle ACFS tagging API, [18-14](#)

acfssettag
Oracle ACFS tagging API, [18-14](#)

acfsutil audit archive command, [16-66](#)

acfsutil audit disable command, [16-67](#)

acfsutil audit enable command, [16-67](#)

acfsutil audit info command, [16-68](#)

acfsutil audit init command, [16-68](#)

acfsutil audit purge command, [16-69](#)

acfsutil audit read command, [16-70](#)

acfsutil detach command, [16-46](#)

acfsutil encr command, [16-102](#)

acfsutil encr info command, [16-100](#)

acfsutil encr init command, [16-101](#)

acfsutil encr off command, [16-101](#)

acfsutil encr rekey command, [16-103](#)

acfsutil encr set command, [16-105](#)

acfsutil info file command, [16-110](#)

acfsutil info fs command, [16-111](#)

acfsutil info id command, [16-115](#)

acfsutil keystore migrate command, [16-106](#)

acfsutil plugin disable command, [16-116](#)

acfsutil plugin enable command, [16-116](#)

acfsutil plugin info command, [16-118](#)

acfsutil registry command, [16-119](#)

acfsutil repl bg command, [16-54](#)

acfsutil repl info command, [16-56](#)

acfsutil repl info compare, [16-55](#)

acfsutil repl init command, [16-58](#)

acfsutil repl pause command, [16-60](#)

acfsutil repl resume command, [16-61](#)

acfsutil repl sync command, [16-62](#)

acfsutil repl terminate command, [16-63](#)

acfsutil repl trace command, [16-64](#)

acfsutil repl update command, [16-64](#)

acfsutil rmfs command, [16-121](#)

acfsutil sec admin add command, [16-72](#)

acfsutil sec admin password command, [16-73](#)

acfsutil sec admin remove command, [16-73](#)

acfsutil sec batch command, [16-74](#)

acfsutil sec disable command, [16-74](#)

acfsutil sec enable command, [16-75](#)

acfsutil sec info command, [16-76](#)

acfsutil sec info file command, [16-77](#)

acfsutil sec init command, [16-77](#)

acfsutil sec load command, [16-79](#)

acfsutil sec prepare command, [16-79](#)

acfsutil sec realm add command, [16-82](#)

- acfsutil sec realm audit disable command, [16-85](#)
- acfsutil sec realm audit enable command, [16-85](#)
- acfsutil sec realm audit info command, [16-87](#)
- acfsutil sec realm clone command, [16-88](#)
- acfsutil sec realm create command, [16-89](#)
- acfsutil sec realm delete command, [16-90](#)
- acfsutil sec realm destroy command, [16-91](#)
- acfsutil sec rule clone command, [16-92](#)
- acfsutil sec rule create command, [16-93](#)
- acfsutil sec rule destroy command, [16-94](#)
- acfsutil sec rule edit command, [16-95](#)
- acfsutil sec ruleset clone command, [16-95](#)
- acfsutil sec ruleset create command, [16-96](#)
- acfsutil sec ruleset destroy command, [16-97](#)
- acfsutil sec ruleset edit command, [16-98](#)
- acfsutil sec save command, [16-98](#)
- acfsutil size command, [16-122](#)
- acfsutil snap convert command, [16-123](#)
- acfsutil snap create command, [16-124](#)
- acfsutil snap delete command, [16-126](#)
- acfsutil snap info command, [16-127](#)
- acfsutil tag info command, [16-50](#)
- acfsutil tag set command, [16-51](#)
- acfsutil tag unset command, [16-53](#)
- acfsutil tune command, [16-129](#)
- active session history sampling
 - Oracle Automatic Storage Management, [3-28](#)
- adding aliases
 - Oracle ASM, [5-13](#)
- adding disks to a disk group, [1-11](#)
- adding disks to a disk group with Oracle Enterprise Manager, [7-8](#)
- adding disks to an Oracle ASM disk group
 - Oracle ASM Configuration Assistant, [9-14](#)
- adding objects to security realms
 - Oracle ACFS, [16-9](#)
- adding security administrators
 - Oracle ACFS file systems, [16-7](#)
- adding templates to a disk group, [5-20](#)
- administering
 - disk groups, [4-1](#)
 - Oracle ACFS, [11-13](#)
- advmutil canonical command, [16-130](#)
- advmutil dismount command, [16-47](#)
- advmutil list command, [16-48](#)
- advmutil mount command, [16-49](#)
- advmutil tune command, [16-131](#)
- advmutil volinfo command, [16-131](#)
- afd_configure command
 - ASMCMD utility, [10-28](#)
- afd_deconfigure command
 - ASMCMD utility, [10-29](#)
- afd_dsget command
 - ASMCMD utility, [10-29](#)
- afd_dsset command
 - ASMCMD utility, [10-30](#)
- afd_filter command
 - ASMCMD utility, [10-30](#)
- afd_filter command (*continued*)
 - ASMCMD utility, [10-30](#)
- afd_label command
 - ASMCMD utility, [10-31](#)
- afd_lsdisk command
 - ASMCMD utility, [10-31](#)
- afd_scan command
 - ASMCMD utility, [10-32](#)
- afd_state command
 - ASMCMD utility, [10-32](#)
- afd_unlabel command
 - ASMCMD utility, [10-33](#)
- AIX
 - Oracle ACFS command-line tools, [16-35](#)
- alias file names
 - Oracle ASM, [5-6](#)
- aliases
 - adding for an Oracle ASM file name, [5-13](#)
 - dropping from a disk group, [5-14](#)
- ALL command rule, [16-83](#)
- allocation units
 - different sizes enabled by compatibility attributes, [4-46](#)
 - Oracle ASM, [1-7](#)
 - size for disk groups, [4-3](#)
- ALTER DISKGROUP command, [4-15](#)
- altering disk groups
 - replacing disks, [4-18](#)
- amdu_extract command
 - ASMCMD utility, [10-34](#)
- APPENDFILE command rule, [16-83](#)
- archive log files
 - creating in Oracle ASM, [17-4](#)
- ASM *See* Oracle Automatic Storage Management
- ASM SPFILE in a disk group
 - enabled by compatibility attributes, [4-47](#)
- ASM_DISKGROUPS initialization parameter
 - Oracle ASM instance, [3-8](#)
- ASM_DISKSTRING initialization parameter
 - discovering disks, [1-11](#)
 - Oracle ASM instance, [3-9](#)
- ASM_POWER_LIMIT initialization parameter
 - Oracle ASM instance, [3-10](#)
 - rebalancing process, [3-10](#)
 - values enabled by compatibility attributes, [4-47](#)
- ASM_PREFERRED_READ_FAILURE_GROUPS
 - initialization parameter
 - Oracle ASM instance, [3-11](#)
- asmadmin group, [3-48](#)
- ASMCA *See* Oracle ASM Configuration Assistant
- ASMCMD utility
 - about, [10-1](#)
 - afd_configure command, [10-28](#)
 - afd_deconfigure command, [10-29](#)
 - afd_dsget command, [10-29](#)
 - afd_dsset command, [10-30](#)
 - afd_filter command, [10-30](#)
 - afd_label command, [10-31](#)

ASMCMD utility (*continued*)

- afd_ksdsk command, [10-31](#)
- afd_scan command, [10-32](#)
- afd_state command, [10-32](#)
- afd_unlabel command, [10-33](#)
- aliases, and, [10-3](#)
- amdu_extract command, [10-34](#)
- cd command, [10-34](#)
- chdg command, [10-45](#)
- chgrp command, [10-68](#)
- chkdg command, [10-46](#)
- chmod command, [10-68](#)
- chown command, [10-70](#)
- chtpl command, [10-64](#)
- command-line utility, [10-1](#), [15-1](#)
- cp command, [10-35](#)
- directories, and, [10-3](#)
- disk group management commands, [10-44](#)
- displaying the version number, [10-9](#)
- dropdg command, [10-47](#)
- dsget command, [10-12](#)
- dsset command, [10-12](#)
- du command, [10-36](#)
- exit command, [10-8](#)
- file access control commands, [10-67](#)
- file management commands, [10-33](#)
- find command, [10-37](#)
- groups command, [10-70](#)
- grpmod command, [10-71](#)
- help command, [10-10](#)
- including directory in prompt, [10-9](#)
- instance management commands, [10-11](#), [10-27](#)
- iostat command, [10-47](#)
- ls command, [10-38](#)
- lsattr command, [10-49](#)
- lsct command, [10-13](#)
- lsdg command, [10-50](#)
- lsdsk command, [10-52](#)
- lsgrp command, [10-72](#)
- lsod command, [10-54](#)
- lsof command, [10-40](#)
- lsop command, [10-14](#)
- lspwusr command, [10-14](#)
- lstmpl command, [10-65](#)
- lsusr command, [10-72](#)
- md_backup command, [10-55](#)
- md_restore command, [10-56](#)
- mkalias command, [10-41](#)
- mkdg command, [10-57](#)
- mkdir command, [10-41](#)
- mkgrp command, [10-73](#)
- mktpl command, [10-66](#)
- mkusr command, [10-74](#)
- mount command, [10-59](#)
- offline command, [10-59](#)
- online command, [10-60](#)

ASMCMD utility (*continued*)

- orapwusr command, [10-15](#)
- passwd command, [10-74](#)
- preparing to run, [10-6](#)
- pwcopy command, [10-16](#)
- pwcreate command, [10-16](#)
- pwd command, [10-42](#)
- pwddelete command, [10-17](#)
- pwget command, [10-18](#)
- pwmove command, [10-19](#)
- pwset command, [10-19](#)
- rebal command, [10-61](#)
- remap command, [10-62](#)
- rm command, [10-42](#)
- rmalias command, [10-43](#)
- rmgrp command, [10-75](#)
- rmtmpl command, [10-66](#)
- rmusr command, [10-75](#)
- rpusr command, [10-76](#)
- running in a database home, [10-7](#)
- running in an Oracle grid infrastructure home, [10-6](#)
- running in interactive mode, [10-7](#)
- running in noninteractive mode, [10-9](#)
- running without any options, [10-8](#)
- setattr command, [10-62](#)
- showclustermode command, [10-20](#)
- showclusterstate command, [10-20](#)
- showpatches command, [10-21](#)
- showversion command, [10-21](#)
- shutdown command, [10-22](#)
- spbackup command, [10-23](#)
- spcopy command, [10-24](#)
- specifying the verbose mode, [10-8](#)
- spget command, [10-25](#)
- spmmove command, [10-25](#)
- spset command, [10-26](#)
- startup command, [10-27](#)
- syntax for starting in interactive mode, [10-7](#)
- SYSASM privilege, [10-8](#)
- system-generated file names, and, [10-2](#)
- template management commands, [10-64](#)
- type of connection, [10-8](#)
- umount command, [10-63](#)
- using quotes for wildcards in noninteractive mode, [10-9](#)
- using with absolute and relative paths, [10-4](#)
- using with wildcard characters, [10-5](#)
- volcreate command, [15-1](#)
- voldelete command, [15-3](#)
- voldisable command, [15-4](#)
- volenable command, [15-5](#)
- volinfo command, [15-5](#)
- volresize command, [15-6](#)
- volset command, [15-7](#)
- volstat command, [15-8](#)
- volume management commands, [15-1](#)

- asmdba group, [3-48](#)
- ASMFDD
 - migrating, [3-36](#)
- asmoper group, [3-48](#)
- ASMSNMP user
 - for monitoring the Oracle ASM instance, [3-47](#)
 - Oracle ASM, [9-2](#)
 - Oracle ASM in Oracle Enterprise Manager, [7-4](#)
- attributes
 - disk group compatibility, [4-41](#)
 - disk groups, [4-2](#)
 - DISK_REPAIR_TIME, [4-34](#)
 - for disk groups, [4-9](#)
 - in templates for Oracle Automatic Storage Management, [5-19](#)
 - list of for disk groups, [4-2](#)
 - setting for disk groups, [4-2](#)
 - viewing for disk groups, [4-2](#)
- AU_SIZE disk group attribute
 - different sizes enabled by compatibility attributes, [4-46](#)
- auditing
 - Oracle ACFS audit trail file, [11-26](#)
 - Oracle ACFS evaluation result events, [11-30](#)
 - Oracle ACFS file access events, [11-27](#)
 - Oracle ACFS privilege use events, [11-28](#)
 - Oracle ACFS security and encryption, [11-24](#)
- authentication
 - operating system with Oracle ASM, [3-51](#)
 - Oracle ASM, [3-46](#)
 - password file with Oracle ASM, [3-51](#)
- Automatic Storage Management
 - home page on Oracle Enterprise Manager, [13-1](#)

B

- backing up Oracle ASM files
 - Oracle Enterprise Manager, [7-27](#)
- backup and restore
 - Oracle ACFS, [11-12](#)
- bad block recovery in Oracle ASM disks
 - Oracle Enterprise Manager, [7-27](#)

C

- capacity
 - managing in disk groups, [4-27](#)
- cd command
 - ASMCMD utility, [10-34](#)
- CELL.SMART_SCAN_CAPABLE disk group attribute, [4-3](#)
- CELL.SPARSE_DG disk group attribute, [4-3](#)
- changing tag names
 - Oracle ACFS, [16-13](#)
- chdg command
 - ASMCMD utility, [10-45](#)
- chgrp command

- chgrp command (*continued*)
 - ASMCMD utility, [10-68](#)
- CHGRP command rule, [16-83](#)
- chkdsk command
 - ASMCMD utility, [10-46](#)
- chmod command
 - ASMCMD utility, [10-68](#)
- CHMOD command rule, [16-83](#)
- chown command
 - ASMCMD utility, [10-70](#)
- CHOWN command rule, [16-83](#)
- chtmp command
 - ASMCMD utility, [10-64](#)
- command rules
 - ALL, [16-83](#)
 - APPENDFILE, [16-83](#)
 - CHGRP, [16-83](#)
 - CHMOD, [16-83](#)
 - CHOWN, [16-83](#)
 - CREATEFILE, [16-83](#)
 - DELETEFILE, [16-83](#)
 - EXTEND, [16-83](#)
 - IMMUTABLE, [16-83](#)
 - LINKFILE, [16-83](#)
 - MKDIR, [16-83](#)
 - MMAPREAD, [16-83](#)
 - MMAPWRITE, [16-83](#)
 - OPENFILE, [16-83](#)
 - Oracle ACFS security, [16-83](#)
 - OVERWRITE, [16-83](#)
 - READ, [16-83](#)
 - REaddir, [16-83](#)
 - RENAME, [16-83](#)
 - RMDIR, [16-83](#)
 - SYMLINK, [16-83](#)
 - TRUNCATE, [16-83](#)
 - WRITE, [16-83](#)
- command utilities
 - Oracle ACFS, [16-107](#)
 - Oracle ACFS for auditing, [16-65](#)
- compatibility
 - disk groups, [4-41](#), [7-8](#)
 - Oracle ASM and database instances, [3-1](#)
 - reverting disk groups to previous settings, [4-45](#)
- COMPATIBLE
 - database initialization parameter, [4-42](#)
- COMPATIBLE.ADVMDisk group attribute
 - default value, [4-42](#)
- COMPATIBLE.ASMDisk group attribute
 - default value, [4-42](#)
- COMPATIBLE.RDBMS disk group attribute
 - default value, [4-42](#)
- components
 - Oracle ASM, [1-2](#)
- concepts
 - Oracle ASM, [1-1](#)
- configuration page

- configuration page (*continued*)
 - Oracle ASM on Oracle Enterprise Manager, [7-3](#)
- configuring an Oracle ASM instance
 - Oracle ASM Configuration Assistant, [9-10](#)
 - Oracle Enterprise Manager, [7-3](#)
- configuring parameters for an Oracle ASM instance
 - Oracle ASM Configuration Assistant, [9-12](#)
- content type of a disk group
 - enabled by compatibility attributes, [4-47](#)
- CONTENT.CHECK disk group attribute, [4-4](#)
- CONTENT.TYPE disk group attribute, [4-4](#)
- control file
 - creating in Oracle ASM, [17-3](#)
- converting snapshots
 - enabled by compatibility attributes, [4-47](#)
- converting to Oracle Flex ASM
 - Oracle ASM Configuration Assistant, [3-30](#), [9-9](#)
- cp command
 - ASMCMD utility, [10-35](#)
- CREATEFILE command rule, [16-83](#)
- creating a database home
 - with Oracle ASMCA, [14-7](#)
- creating a database using Oracle ASM, [17-1](#)
- creating a new directory
 - Oracle ASM, [5-15](#)
- creating an Oracle ACFS file system
 - Oracle ASM Configuration Assistant, [14-10](#)
- creating an Oracle ADVM volume
 - Oracle ASM Configuration Assistant, [14-9](#)
- creating an Oracle ASM disk group
 - Oracle ASM Configuration Assistant, [9-13](#)
- creating disk groups, [4-7](#)
- creating disk groups and adding disks, [4-8](#)
- creating disk groups and attributes, [4-8](#)
- creating disk groups and failure group types, [4-8](#)
- creating disk groups and failure groups, [4-8](#)
- creating disk groups and redundancy level, [4-7](#)
- creating disk groups in a new installation, [4-10](#)
- creating files in the database
 - Oracle ASM, [5-8](#)
- creating files using a default file location
 - Oracle ASM, [5-8](#)
- creating from existing snapshots
 - enabled by compatibility attributes, [4-47](#)
- creating Oracle ACFS file systems, [16-3](#)
- creating security realms
 - Oracle ACFS, [16-8](#)
- creating security rule sets
 - Oracle ACFS, [16-9](#)
- creating security rules
 - Oracle ACFS, [16-8](#)

D

- data files
 - moving between disk groups, [5-10](#)
- data files with alias names

- data files with alias names (*continued*)
 - Oracle ASM, [5-6](#)
- database files
 - Oracle ACFS on Oracle Exadata, [11-6](#)
- DB_CACHE_SIZE initialization parameter
 - Oracle ASM instance, [3-11](#)
- default configuration
 - Oracle ADVM, [15-3](#), [18-3](#)
- DELETEFILE command rule, [16-83](#)
- deleting Oracle ASM instances
 - Oracle ASM Configuration Assistant, [9-12](#)
- deregistering file systems
 - Oracle ACFS, [16-20](#)
- determining the volume device name
 - Oracle ACFS, [16-2](#)
- diagnostic directory
 - Oracle ASM instance, [3-12](#)
- DIAGNOSTIC_DEST initialization parameter
 - Oracle ASM instance, [3-12](#)
- directories
 - ACFS for snapshots, [11-10](#), [16-125](#)
 - creating disk group, [5-15](#)
 - dropping disk group, [5-16](#)
 - managing disk group, [5-14](#)
 - Oracle ASM, [5-14](#)
 - renaming disk group, [5-15](#)
- disabling a volume
 - Oracle ACFS, [16-20](#)
- disk discovery
 - about, [4-25](#)
 - improving time, [4-27](#)
 - in Oracle ASM, [4-25](#)
 - Oracle ASM, [1-11](#)
 - rules, [4-26](#)
- disk failures
 - in Oracle Automatic Storage Management, [4-32](#)
- disk group compatibility
 - configuring with Oracle Enterprise Manager, [7-16](#)
 - considerations for replicated environments, [4-48](#)
 - considerations in a replicated environments, [4-48](#)
 - Oracle ACFS features enabled by settings, [4-47](#)
 - Oracle ASM features enabled by settings, [4-46](#)
 - setting, [4-42](#)
 - setting in Oracle Enterprise Manager, [7-8](#)
 - setting with ALTER DISKGROUP, [4-44](#)
 - setting with CREATE DISKGROUP, [4-44](#)
 - valid combinations, [4-43](#)
 - viewing compatibility settings, [4-45](#)
- disk group management commands
 - ASMCMD utility, [10-44](#)
- disk group properties
 - configuring with Oracle Enterprise Manager, [7-15](#)
- disk group repair time
 - configuring with Oracle Enterprise Manager, [7-16](#)
- disk group smart scan compatibility
 - configuring with Oracle Enterprise Manager, [7-16](#)
- disk groups

disk groups (*continued*)

- access control, [4-49](#)
- ACCESS_CONTROL.ENABLED attribute, [4-51](#)
- ACCESS_CONTROL.UMASK attribute, [4-51](#)
- adding disks to with Oracle ASM Configuration Assistant, [9-14](#)
- adding disks to with Oracle Enterprise Manager, [7-8](#)
- adding templates to, [5-20](#)
- administering, [4-1](#)
- allocation unit size, [4-3](#)
- altering membership of, [4-15](#)
- attributes, [4-2](#), [4-9](#)
- checking internal consistency, [4-55](#)
- compatibility, [4-41](#)
- compatibility attributes, [4-41](#)
- creating, [4-7](#)
- creating and adding disks, [4-8](#)
- creating and attributes, [4-8](#)
- creating and failure group types, [4-8](#)
- creating and failure groups, [4-8](#)
- creating and redundancy level, [4-7](#)
- creating for a new installation, [4-10](#)
- creating Oracle Enterprise Manager, [7-6](#)
- creating with Oracle ASM Configuration Assistant, [9-13](#)
- creating with SQL*Plus, [4-7](#)
- determining the number of, [4-38](#)
- directories, [5-14](#)
- discovering disks, [4-25](#)
- dismounting, [1-11](#)
- dismounting with Oracle Enterprise Manager, [7-14](#)
- dropping, [4-56](#)
- dropping disks from, [4-19](#)
- dropping disks with Oracle Enterprise Manager, [7-11](#)
- dropping in Oracle Enterprise Manager, [7-13](#)
- even read, [4-36](#)
- failure groups, [4-30](#), [4-31](#)
- list of attributes, [4-2](#)
- managing a shared password file, [3-52](#)
- managing capacity in, [4-27](#)
- manually rebalancing, [4-21](#)
- mirroring, [4-30](#)
- monitoring disk space usage in Oracle Enterprise Manager, [7-14](#)
- mounting, [1-11](#)
- mounting and dismounting, [4-54](#)
- mounting at startup, [3-24](#)
- mounting with force, [4-54](#)
- mounting with Oracle Enterprise Manager, [7-14](#)
- moving data files between, [5-10](#)
- names, [4-7](#)
- Oracle ASM, [1-5](#)
- Oracle Cluster Registry (OCR), and, [4-13](#)
- performance and scalability, [4-38](#)

disk groups (*continued*)

- performance characteristics when grouping disks, [4-39](#)
- preferred read, [3-11](#)
- quorum failure groups, [4-13](#)
- rebalancing, [1-12](#)
- redundancy, [4-30](#)
- renamedg, [4-57](#)
- renaming, [4-57](#)
- renaming disks, [4-18](#)
- replacing disks, [4-18](#)
- resizing disks in, [4-21](#)
- reverting compatibility, [4-45](#)
- scrubbing, [4-24](#)
- sector size, [4-11](#)
- setting attributes, [4-2](#)
- storage limits, [4-39](#)
- tracking the replication status, [4-5](#)
- undropping disks in, [4-21](#)
- validations for sector size, [4-12](#)
- viewing attributes, [4-2](#)
- voting files, and, [4-13](#)
- when to use external, normal, or high redundancy, [4-33](#)

disk partitions

- storage resources, [2-1](#)

disk regions

- intelligent data placement, [4-20](#)
- Oracle Automatic Storage Management, [4-20](#)
- rebalance operations, and, [4-20](#)

DISK_REPAIR_TIME disk group attribute

- fast disk resync, [4-34](#)

disks

- adding to a disk group, [1-11](#)
- discovering, [1-11](#), [4-25](#)
- dropping from a disk group, [1-11](#)
- Oracle ASM, [1-6](#)
- regions, [4-20](#)

dismounting disk groups, [1-11](#)

dismounting file systems

- Oracle ACFS, [16-20](#)

dismounting or shutting down

- Oracle ACFS, [11-19](#)

displaying encryption information

- Oracle ACFS, [16-12](#)

displaying security information

- Oracle ACFS, [16-10](#)

displaying tagging information

- Oracle ACFS, [16-13](#)

driver commands

- acfsdriverstate, [18-6](#)
- acfsload, [18-5](#)
- Oracle ACFS, [18-5](#)

driver model

- Oracle ACFS, [11-9](#)

drivers resource

- Oracle ACFS, [18-4](#)

- dropdg command
 - ASMCMD utility, [10-47](#)
- dropping a directory
 - Oracle ASM, [5-16](#)
- dropping aliases
 - Oracle ASM, [5-14](#)
- dropping aliases from a disk group, [5-14](#)
- dropping disk groups, [4-56](#)
- dropping disks from a disk group, [1-11](#), [4-19](#)
- dropping disks from disk groups in Oracle Enterprise Manager, [7-11](#)
- dropping files from a disk group
 - Oracle ASM, [5-14](#)
- dropping Oracle ASM templates, [5-21](#)
- dsget command
 - ASMCMD utility, [10-12](#)
- dsset command
 - ASMCMD utility, [10-12](#)
- du command
 - ASMCMD utility, [10-36](#)
- dynamic views, [6-1](#), [12-1](#)

E

- enabling encryption
 - Oracle ACFS, [16-12](#)
- encrypting file systems
 - Oracle ACFS, [16-11](#)
- encrypting secure file systems
 - Oracle ACFS, [16-8](#)
- encryption
 - configuring with Oracle ASMCA, [14-5](#)
 - enabled by compatibility attributes, [4-47](#)
 - Oracle ACFS, [11-22](#)
 - Oracle ACFS and snapshots, [11-11](#)
- encryption keys
 - Oracle ACFS, [11-22](#)
- Enterprise Manager *See* Oracle Enterprise Manager
- Enterprise Manager Cloud Control *See* Oracle Enterprise Manager
- error handling
 - Oracle ACFS, [18-2](#)
- even read
 - disk groups, [4-36](#)
 - distributing data reads, [4-36](#)
- Exadata storage
 - enabled by compatibility attributes, [4-46](#)
- exit command
 - ASMCMD utility, [10-8](#)
- EXTEND command rule, [16-83](#)
- Extended Attributes
 - requirements for tagging, [11-33](#)
- extents
 - Oracle ASM, [1-7](#), [1-8](#)
 - variable size, [1-7](#), [1-8](#), [4-29](#), [4-46](#)
- external tables
 - and Oracle ACFS, [11-13](#)

F

- FAILGROUP_REPAIR_TIME disk group attribute
 - fast disk resync, [4-36](#)
- failure groups
 - about, [4-31](#)
 - disk failures, [4-32](#)
 - guidelines, [4-32](#)
 - how many to create, [4-32](#)
 - minimum recommended, [4-31](#)
 - mirroring, and, [4-30](#)
 - Oracle ASM, [1-5](#)
 - preferred read, [4-37](#)
 - quorum type, [4-13](#)
 - simultaneous failure, [4-33](#)
 - when to use external, normal, or high redundancy, [4-33](#)
- fast mirror resync
 - enabled by compatibility attributes, [4-46](#)
 - managing with Oracle Enterprise Manager, [7-10](#), [7-11](#)
- file access and security
 - Oracle ACFS, [11-13](#)
- file access control
 - enabled by compatibility attributes, [4-47](#)
 - enabling with Oracle Enterprise Manager, [7-17](#)
 - managing with SQL statements, [4-51](#)
 - Oracle Automatic Storage Management, [4-49](#)
 - restricting access to files, [4-49](#)
 - setting up for files in a disk group, [4-50](#)
 - setting with SQL statements, [4-50](#)
- file management commands
 - ASMCMD utility, [10-33](#)
- file names
 - Oracle ASM, [5-2](#)
 - Oracle Automatic Storage Management, [5-2](#)
- file names in SQL statements
 - Oracle ASM, [5-9](#)
- file names with template form
 - Oracle ASM, [5-7](#)
- file templates
 - understanding, [1-10](#)
- file types supported
 - Oracle ASM, [5-1](#)
- files
 - Oracle ASM, [1-7](#)
 - templates, [1-10](#)
- filter driver
 - Oracle ASM, [3-34](#)
- find command
 - ASMCMD utility, [10-37](#)
- fsck command
 - AIX, [16-35](#)
 - Linux environments, [16-22](#)
 - Solaris, [16-29](#)
- fully qualified file names
 - Oracle ASM, [5-4](#)

G

- greater than 2 TB Oracle ASM disks
 - enabled by compatibility attributes, [4-47](#)
- grid infrastructure configuration
 - Oracle ACFS, [11-14](#)
- grid infrastructure installation
 - Oracle ACFS, [11-14](#)
- grid plug and play (GPnP)
 - retrieving the location of an ASM SPFILE, [10-25](#)
 - setting the location of the ASM SPFILE, [10-26](#)
- groups
 - OSASM, [3-46](#), [3-50](#), [3-51](#)
- groups command
 - ASMCMD utility, [10-70](#)
- grpmod command
 - ASMCMD utility, [10-71](#)

H

- help command
 - ASMCMD utility, [10-10](#)
- High Availability NFS for Oracle Grid Home
 - notes, [11-37](#)
 - Oracle ACFS, [11-36](#)
 - setting up for an Oracle ACFS file system, [11-37](#)

I

- I/O failure console messages
 - Oracle ACFS, [18-15](#)
- IDP.BOUNDARY disk group attribute, [4-5](#)
- IDP.TYPE disk group attribute, [4-5](#)
- IMMUTABLE command rule, [16-83](#)
- incomplete file name form
 - Oracle ASM, [5-7](#)
- incomplete file name template form
 - Oracle ASM, [5-8](#)
- individual file system resource
 - Oracle ACFS, [18-4](#)
- initialization parameter files
 - backing up, copying, and moving, [3-4](#)
 - creating an SPFILE in a disk group, [3-5](#)
 - Oracle ASM, [3-3](#)
 - search order for Oracle ASM, [3-3](#)
- initialization parameters
 - COMPATIBLE, [4-42](#)
 - database for use with Oracle ASM instance, [3-14](#)
 - Oracle ASM instance, [3-8](#)
 - Oracle Automatic Storage Management, [3-2](#)
 - setting for Oracle ASM instance, [3-6](#)
- initializing encryption on file systems
 - Oracle ACFS, [16-11](#)
- initializing security
 - Oracle ACFS file systems, [16-6](#)
- instance management commands
 - ASMCMD utility, [10-11](#), [10-27](#)
- INSTANCE_TYPE initialization parameter

- INSTANCE_TYPE initialization parameter (*continued*)
 - Oracle ASM instance, [3-12](#)
- instances
 - Oracle ASM, [1-3](#)
- intelligent data placement
 - disk regions, [4-20](#)
 - enabled by compatibility attributes, [4-46](#)
 - rebalance operations, and, [4-20](#)
- iostat command
 - ASMCMD utility, [10-47](#)

K

- keys
 - encryption, [11-22](#)

L

- LARGE_POOL_SIZE initialization parameter
 - Oracle ASM instance, [3-12](#)
- limits
 - Oracle ACFS, [18-1](#)
 - Oracle ADVM, [18-3](#)
- LINKFILE command rule, [16-83](#)
- Linux environments
 - Oracle ACFS command-line tools, [16-21](#)
- logical unit number
 - storage resources, [2-1](#)
- logical volumes
 - storage resources, [2-1](#)
- ls command
 - ASMCMD utility, [10-38](#)
- lsattr command
 - ASMCMD utility, [10-49](#)
- lsct command
 - ASMCMD utility, [10-13](#)
- lsdg command
 - ASMCMD utility, [10-50](#)
- lsdsk command
 - ASMCMD utility, [10-52](#)
- lsgrp command
 - ASMCMD utility, [10-72](#)
- lsod command
 - ASMCMD utility, [10-54](#)
- lsnf command
 - ASMCMD utility, [10-40](#)
- lsop command
 - ASMCMD utility, [10-14](#)
- lspwusr command
 - ASMCMD utility, [10-14](#)
- lstmpl command
 - ASMCMD utility, [10-65](#)
- lsusr command
 - ASMCMD utility, [10-72](#)

M

- managing a shared password file in a disk group

- managing a shared password file in a disk group (*continued*)
 - enabled by compatibility attributes, [4-47](#)
- managing aliases
 - Oracle ASM, [5-13](#)
- managing capacity in disk groups, [4-27](#)
- managing file access control
 - Oracle Enterprise Manager, [7-21](#)
- managing file access control for disk groups
 - Oracle Enterprise Manager, [7-21](#)
- managing Oracle ASM files
 - Oracle Enterprise Manager, [7-22](#)
- managing Oracle ASM templates
 - Oracle Enterprise Manager, [7-23](#)
- managing Oracle ASM templates page
 - Oracle Enterprise Manager, [7-23](#)
- managing templates
 - Oracle Automatic Storage Management, [5-18](#)
- managing users
 - Oracle ASM in Oracle Enterprise Manager, [7-4](#)
- md_backup command
 - ASMCMD utility, [10-55](#)
- md_restore command
 - ASMCMD utility, [10-56](#)
- memory management
 - Oracle Automatic Storage Management, [3-7](#)
- migrating a database
 - to Oracle ASM, [3-54](#)
- migrating data
 - Oracle ASM with Recovery Manager, [8-1](#)
- migrating data to alternative storage
 - Oracle ASM, [8-9](#)
- migrating data to Oracle ASM
 - with Recovery Manager, [8-5](#)
- migrating to Oracle ASM
 - Oracle Enterprise Manager, [7-28](#)
- mirror
 - fast resync, [4-34](#), [7-10](#), [7-11](#)
- mirroring
 - failure groups, and, [4-30](#)
 - Oracle ASM, [1-5](#)
 - with failure groups, [1-5](#)
- mkalias command
 - ASMCMD utility, [10-41](#)
- mkdg command
 - ASMCMD utility, [10-57](#)
- mkdir command
 - ASMCMD utility, [10-41](#)
- MKDIR command rule, [16-83](#)
- mkfs command
 - AIX, [16-37](#)
 - Linux environments, [16-24](#)
 - Solaris, [16-30](#)
- mkgrp command
 - ASMCMD utility, [10-73](#)
- mktpl command
 - ASMCMD utility, [10-66](#)
- mkusr command
 - ASMCMD utility, [10-74](#)

- MMAPREAD command rule, [16-83](#)
- MMAPWRITE command rule, [16-83](#)
- modifying a file
 - disk regions, [4-20](#)
- monitoring Oracle ASM performance
 - Oracle Enterprise Manager, [7-26](#)
- mount command
 - AIX, [16-38](#)
 - ASMCMD utility, [10-59](#)
 - Linux environments, [16-26](#)
 - Solaris, [16-32](#)
- mount model
 - Oracle ACFS, [11-5](#)
- mount registry
 - Oracle ACFS, [11-9](#)
- mounting and dismounting disk groups, [4-54](#)
- mounting disk groups
 - using force, [4-54](#)
- mounting Oracle ACFS file systems, [16-4](#)
- moving data between disk groups
 - Oracle ASM, [8-9](#)
- multipathing
 - with Oracle ASM, [2-3](#)
- multiple file creation form
 - Oracle ASM, [5-4](#)

N

- namespace
 - Oracle ACFS, [11-5](#)
- naming
 - disk groups, [4-7](#)
- network file systems
 - storage resources, [2-2](#)
- NFS
 - and Oracle ACFS, [18-3](#)
- NOWAIT keyword
 - in REBALANCE clause, [4-15](#)

O

- OCR in disk groups
 - enabled by compatibility attributes, [4-46](#)
- offline command
 - ASMCMD utility, [10-59](#)
- online command
 - ASMCMD utility, [10-60](#)
- open files
 - and chgrp command, [10-68](#)
 - and chmod command, [10-69](#)
 - and chown command, [10-70](#)
- OPENFILE command rule, [16-83](#)
- operating system authentication
 - for Oracle Automatic Storage Management, [3-51](#)
 - Oracle ASM, [3-51](#)
 - SYSASM, [3-51](#)
- ora.diskgroup.volume.acfs file system resource

- ora.diskgroup.volume.acfs file system resource (*continued*)
 - Oracle ACFS, [11-16](#)
- ora.drivers.acfs drivers resource
 - Oracle ACFS, [11-15](#)
- Oracle ACFS *See* Oracle Automatic Storage Management Cluster File System
- Oracle ACFS security
 - command rules, [16-83](#)
- Oracle ADVM *See* Oracle Automatic Storage Management Dynamic Volume Manager
- Oracle ADVM volume devices
 - creating, [16-2](#)
- Oracle ASM *See* Oracle Automatic Storage Management
- Oracle ASM Configuration Assistant
 - about, [9-1, 14-1](#)
 - addDisk command, [9-14](#)
 - commands, [9-9, 14-9](#)
 - configureASM command, [9-10](#)
 - configureParameter command, [9-12](#)
 - configuring an Oracle ACFS, [14-3](#)
 - configuring an Oracle ADVM volume, [14-1](#)
 - configuring disk groups, [9-5](#)
 - configuring Oracle ACFS encryption, [14-5](#)
 - configuring Oracle ACFS for a database home, [14-7](#)
 - configuring Oracle ACFS security, [14-5](#)
 - converting to Oracle Flex ASM, [3-30](#)
 - convertToFlexASM command, [9-9](#)
 - createACFS command, [14-10](#)
 - createDiskGroup command, [9-13](#)
 - createVolume command, [14-9](#)
 - creating a database home on Oracle ACFS, [14-7](#)
 - creating an Oracle ACFS file system, [14-4](#)
 - creating an Oracle ADVM volume, [14-1](#)
 - creating an Oracle ASM instance, [9-2](#)
 - creating disk groups, [9-6](#)
 - deleteASM command, [9-12](#)
 - mounting or dismounting an Oracle ACFS, [14-3](#)
 - running in command-line mode, [9-8](#)
 - running in silent mode, [9-8](#)
 - starting, [9-1](#)
 - updating Oracle ASM instance parameters, [9-3](#)
 - upgradeASM command, [9-11](#)
 - upgrading an Oracle ASM instance, [9-4](#)
- Oracle ASM Dynamic Volume Manager
 - overview, [11-1](#)
- Oracle ASM file access control commands
 - ASMCMD utility, [10-67](#)
- Oracle ASM Filter Driver
 - about, [3-34](#)
 - and Oracle ASMLIB, [3-35](#)
 - configuring, [3-36](#)
 - deconfiguring, [3-43](#)
 - determining the state, [3-41](#)
 - managing labels, [3-42](#)
 - managed by Oracle Enterprise Manager, [7-23](#)
 - migrating, [3-36, 3-38](#)
 - updating AFD_DISKSTRING, [3-41](#)
- Oracle ASM Filter Driver (*continued*)
 - updating ASM_DISKSTRING, [3-42](#)
- Oracle ASM performance
 - Oracle Enterprise Manager, [7-26](#)
- Oracle ASM preferred read
 - failure groups, [4-37](#)
- Oracle ASM proxy instance
 - Oracle ACFS and Oracle ADVM, [3-17](#)
- Oracle Automatic Storage Management
 - accessing files with the XML DB virtual folder, [5-16](#)
 - active session history sampling, [3-28](#)
 - adding aliases, [5-13](#)
 - administering, [3-1](#)
 - administering Oracle Flex ASM, [3-19](#)
 - alias file names, [5-6](#)
 - aliases, [5-13](#)
 - and Oracle Enterprise Manager, [7-1](#)
 - ASM_POWER_LIMIT initialization parameter, [3-10](#)
 - ASM_PREFERRED_READ_FAILURE_GROUPS initialization parameter, [3-11](#)
 - ASMSNMP, [9-2](#)
 - ASMSNMP user in Oracle Enterprise Manager, [7-4](#)
 - authentication, [3-46](#)
 - backing up initialization parameter files, [3-4](#)
 - command-line utility, [10-1, 15-1](#)
 - components, [1-2](#)
 - concepts, [1-1](#)
 - configuring initialization parameters, [3-2](#)
 - connecting to an instance, [3-22](#)
 - converting to Oracle Flex ASM, [3-30](#)
 - copying initialization parameter files, [3-4](#)
 - creating a database example, [17-1](#)
 - creating a database in, [17-1](#)
 - creating a new directory, [5-15](#)
 - creating archive log files in, [17-4](#)
 - creating control file example, [17-3, 17-4](#)
 - creating control file in, [17-3](#)
 - creating files in the database, [5-8](#)
 - creating files using a default file location, [5-8](#)
 - creating redo logs in, [17-2](#)
 - creating SPFILE in a disk group, [3-5](#)
 - creating tablespaces in, [17-2](#)
 - data files with alias names, [5-6](#)
 - database initialization parameters, [3-14](#)
 - DB_CACHE_SIZE initialization parameter, [3-11](#)
 - diagnostic directory, [3-12](#)
 - DIAGNOSTIC_DEST initialization parameter, [3-12](#)
 - directories, [5-14](#)
 - discovering disks, [1-11, 4-25](#)
 - disk discovery, [4-25](#)
 - disk discovery string, [1-11](#)
 - disk failures in, [4-32](#)
 - disk groups, [1-5](#)
 - disk partitions for storage resources, [2-1](#)
 - disk regions, [4-20](#)

Oracle Automatic Storage Management (*continued*)

- disks, [1-6](#)
- dropping a directory, [5-16](#)
- dropping aliases, [5-14](#)
- dropping files, [5-14](#)
- extents, [1-8](#)
- failure groups, [4-31](#)
- failure groups recommendations, [4-31](#)
- file access control, [4-49](#)
- file names, [5-2](#)
- file names with template form, [5-7](#)
- file templates, [1-10](#)
- file types supported, [5-1](#)
- files, [1-7](#)
- fully qualified file names, [5-4](#)
- home page on Oracle Enterprise Manager, [7-1](#)
- incomplete file name form, [5-7](#)
- incomplete file name template form, [5-8](#)
- initialization parameter files, [3-3](#)
- initialization parameters, [3-8](#)
- INSTANCE_TYPE initialization parameter, [3-12](#)
- instances, [1-3](#)
- integration with Oracle ACFS, [11-12](#)
- LARGE_POOL_SIZE initialization parameter, [3-12](#)
- logical volumes for storage resources, [2-1](#)
- LUNs for storage resources, [2-1](#)
- managing aliases, [5-13](#)
- memory management, [3-7](#)
- migrating a database to, [3-54](#)
- migrating data, [8-1](#), [8-2](#)
- migrating data to, [8-5](#)
- migrating data to alternative storage, [8-9](#)
- mirroring and failure groups, [1-5](#)
- moving data between disk groups, [8-9](#)
- moving initialization parameter files, [3-4](#)
- multipathing, [2-3](#)
- multiple file creation form, [5-4](#)
- network file systems for storage resources, [2-2](#)
- one operating system group for all privileges, [3-47](#)
- operating system authentication for, [3-51](#)
- Oracle Database file mapping, [5-10](#)
- Oracle Flex ASM, [3-15](#), [3-16](#)
- ORACLE_HOME, [3-22](#)
- ORACLE_SID, [3-22](#)
- overview, [1-1](#)
- password file authentication for, [3-51](#)
- preparing storage resources, [2-2](#)
- privileges, [3-47](#)
- PROCESSES initialization parameter, [3-13](#)
- recommendations for storage preparation, [2-4](#)
- Recovery Manager, and, [8-1](#), [8-2](#)
- referencing files in the database, [5-8](#)
- REMOTE_LOGIN_PASSWORDFILE initialization parameter, [3-13](#)
- renaming a directory, [5-15](#)
- renaming aliases, [5-13](#)

Oracle Automatic Storage Management (*continued*)

- rolling patches, [3-30](#)
- rolling upgrades, [3-29](#)
- search order for initialization parameter files, [3-3](#)
- separate operating system groups for privileges, [3-48](#)
- setting initialization parameters, [3-6](#)
- setting up Oracle Flex ASM, [3-18](#)
- SHARED_POOL_SIZE initialization parameter, [3-14](#)
- shutting down an instance, [3-25](#)
- shutting down an instance with OCR or voting files in a disk group, [3-25](#)
- shutting down an instance with Oracle ACFS, [3-26](#)
- single file creation form, [5-4](#)
- starting up an instance, [3-22](#)
- starting up an instance with incorrect SPFILE path, [3-24](#)
- storage considerations, [2-1](#)
- storage limits, [4-39](#)
- storage resources, [2-1](#)
- striping, [1-9](#)
- upgrading an instance with Oracle ASM Configuration Assistant, [9-4](#)
- users page in Oracle Enterprise Manager, [7-4](#)
- using file names in SQL statements, [5-9](#)
- views, [6-1](#)
- XML DB virtual folder, [5-16](#)

Oracle Automatic Storage Management Cluster File System

- about, [11-4](#)
- accelerator volume, [16-25](#)
- adding objects to security realms, [16-9](#)
- adding security administrators, [16-7](#)
- administering, [11-13](#)
- and external tables on Windows, [11-13](#)
- and NFS, [18-3](#)
- and Oracle Enterprise Manager, [13-1](#)
- and Oracle Restart, [18-5](#)
- auditing files and Oracle Database homes, [11-8](#)
- auditing security and encryption, [11-24](#)
- backup and restore, [11-12](#)
- basic steps to access a file system, [16-4](#)
- basic steps to create a file system, [16-2](#)
- basic steps to deregister, dismount, and disable a volume and file system, [16-19](#)
- basic steps to manage snapshots, [16-5](#)
- basic steps to manage with command-line tools, [16-1](#)
- basic steps to remove a file system and volume, [16-21](#)
- changing tag names, [16-13](#)
- command-line tools, [16-1](#)
- creating file systems, [16-3](#)
- creating security realms, [16-8](#)
- creating security rule sets, [16-9](#)

- Oracle Automatic Storage Management Cluster File System (*continued*)
- creating security rules, [16-8](#)
 - creating snapshots with Oracle Enterprise Manager, [13-6](#)
 - creating volumes and file systems with Oracle Enterprise Manager, [13-2](#)
 - database files with Oracle Exadata, [11-6](#)
 - deregistering file systems, [16-20](#)
 - determining the Oracle ADVM volume device name, [16-2](#)
 - disabling a volume, [16-20](#)
 - disk group compatibility, [16-2](#)
 - dismount or shut down, [11-19](#)
 - dismounting file systems, [16-20](#)
 - displaying encryption information, [16-12](#)
 - displaying security information, [16-10](#)
 - displaying tagging information, [16-13](#)
 - driver commands, [18-5](#)
 - driver model, [11-9](#)
 - drivers resource, [18-4](#)
 - enabling encryption, [16-12](#)
 - encrypting file systems, [16-11](#)
 - encrypting secure file systems, [16-8](#)
 - encryption, [11-22](#)
 - encryption keys, [11-22](#)
 - error handling, [18-2](#)
 - file access and security, [11-13](#)
 - file mapping, [12-6](#)
 - file systems on other nodes, [16-4](#)
 - grid infrastructure configuration, [11-14](#)
 - grid infrastructure installation, [11-14](#)
 - High Availability NFS for Oracle Grid Home, [11-36](#)
 - I/O failure console messages, [18-15](#)
 - important considerations with database files, [11-5](#)
 - important general considerations, [11-3](#)
 - individual file system resource, [18-4](#)
 - initializing encryption on file systems, [16-11](#)
 - initializing security on file systems, [16-6](#)
 - integration with Oracle ASM, [11-12](#)
 - limit on the number of snapshots, [18-2](#)
 - limits, [18-1](#)
 - mount model, [11-5](#)
 - mount point and Oracle Database homes, [11-7](#)
 - mount registry, [11-9](#)
 - mounting file systems, [16-4](#)
 - namespace, [11-5](#)
 - ora.diskgroup.volume.acfs file system resource, [11-16](#)
 - ora.drivers.acfs drivers resource, [11-15](#)
 - Oracle ADVM, [11-39](#)
 - Oracle ADVM volume devices, [16-2](#)
 - Oracle ASM proxy instance, [3-17](#)
 - Oracle Clusterware resource types, [11-14](#)
 - Oracle Database homes, and, [11-7](#)
 - overview, [1-2](#), [11-1](#)
- Oracle Automatic Storage Management Cluster File System (*continued*)
- plug-in API, [18-7](#)
 - plugins, [11-36](#)
 - preparing security on file systems, [16-7](#)
 - read-only and read-write snapshots, [11-10](#)
 - read-write snapshots, [11-10](#)
 - registering file systems, [16-3](#)
 - registry resource, [18-4](#)
 - removing tag names, [16-13](#)
 - replicating file systems, [16-13](#)
 - replication, [11-30](#)
 - replication with auditing, encryption, and security, [11-35](#)
 - restrictions for storage resource, [2-2](#)
 - saving security information, [16-10](#)
 - securing file systems, [16-6](#)
 - security, [11-19](#)
 - setting encryption parameters, [16-11](#)
 - snapshots, [16-124](#), [16-126](#), [16-127](#)
 - space usage, [18-2](#)
 - specifying tag names for file systems, [16-12](#)
 - supported file types, [11-1](#)
 - system-created security realms, [16-80](#)
 - tagging, [11-33](#)
 - tagging API, [18-10](#)
 - tagging file systems, [16-12](#)
 - viewing and modifying snapshots with Oracle Enterprise Manager, [13-5](#)
 - viewing and modifying volumes and file systems with Oracle Enterprise Manager, [13-3](#)
 - views, [12-1](#)
- Oracle Automatic Storage Management Dynamic Volume Manager
- accelerator volume, [16-25](#)
 - default configuration, [15-3](#), [18-3](#)
 - limits, [18-3](#)
 - Oracle ACFS, [11-39](#)
 - overview, [11-9](#), [11-39](#)
- Oracle Cluster Registry (OCR)
- in disk groups, [4-13](#)
- Oracle Clusterware resource types
- Kernel Services Driver (OKS), [11-14](#)
 - Oracle ACFS, [11-14](#)
 - Oracle ADVM, [11-14](#)
- Oracle Database file mapping
- with Oracle ACFS, [12-6](#)
 - with Oracle ASM, [5-10](#)
- Oracle Database homes
- Oracle ACFS, and, [11-7](#)
- Oracle Enterprise Manager
- accessing the Oracle ASM home page, [7-1](#), [13-1](#)
 - adding disks to a disk group, [7-8](#)
 - and Oracle ACFS, [13-1](#)
 - and Oracle ASM, [7-1](#)
 - backing up Oracle ASM files, [7-27](#)
 - bad block recovery in Oracle ASM disks, [7-27](#)

- Oracle Enterprise Manager (*continued*)
 - creating disk groups, [7-6](#)
 - creating Oracle ACFS file systems, [13-2](#)
 - creating Oracle ACFS snapshots, [13-6](#)
 - creating Oracle ACFS volumes, [13-2](#)
 - disk group compatibility, [7-16](#)
 - disk group file access control, [7-17](#)
 - disk group properties, [7-15](#)
 - disk group repair time, [7-16](#)
 - disk group smart scan compatibility, [7-16](#)
 - dismounting disk groups, [7-14](#)
 - dropping disk groups, [7-13](#)
 - dropping disks from disk groups, [7-11](#)
 - managing fast mirror resync, [7-10](#)
 - managing file access control for disk groups, [7-21](#)
 - managing Oracle ASM files, [7-22](#)
 - managing Oracle ASM Filter Driver, [7-23](#)
 - managing Oracle ASM templates, [7-23](#)
 - migrating to Oracle ASM, [7-28](#)
 - monitoring Oracle ASM disk group space usage, [7-14](#)
 - mounting disk groups, [7-14](#)
 - Oracle ASM configuration page, [7-3](#)
 - Oracle ASM performance page, [7-26](#)
 - Oracle ASM users page, [7-4](#)
 - setting disk group compatibility, [7-8](#)
 - support workbench for Oracle ASM, [7-29](#), [7-31](#)
 - viewing and modifying Oracle ACFS snapshots, [13-5](#)
 - viewing and modifying Oracle ACFS volumes and file systems, [13-3](#)
- Oracle Flex ASM
 - administering, [3-19](#)
 - configuring, [3-18](#)
 - converting to, [3-30](#)
 - database clients, [3-16](#)
 - direct Oracle ASM clients, [3-17](#)
 - INSTANCE_TYPE initialization parameter, [3-17](#)
 - local Oracle ASM clients, [3-17](#)
 - multiple Oracle ASM instances, [3-16](#)
 - Oracle ASM proxy instance, [3-17](#)
 - overview, [3-16](#)
 - relocating clients, [3-20](#)
 - setting up, [3-18](#)
- Oracle Home user on Windows
 - lower privileged user, [3-28](#)
- Oracle Restart
 - about, [3-21](#)
 - and Oracle ACFS, [18-5](#)
 - standalone server, [3-21](#)
 - with Oracle ASM, [3-21](#)
- ORACLE_HOME
 - Oracle ASM, [3-22](#)
- ORACLE_SID
 - Oracle ASM, [3-22](#)
- orapwusr command

- orapwusr command (*continued*)
 - ASMCMD utility, [10-15](#)
- OSASM group, [3-46](#), [3-48](#), [3-50](#), [3-51](#)
- OSDBA group, [3-48](#)
- OSOPER group, [3-48](#)
- OSTMG10048, [4-25](#)
- overview
 - Oracle ACFS, [1-2](#), [11-1](#)
 - Oracle ACFS and Oracle ADVM, [11-1](#)
 - Oracle ADVM, [11-9](#)
 - Oracle ASM, [1-1](#)
- OVERWRITE command rule, [16-83](#)

P

- passwd command
 - ASMCMD utility, [10-74](#)
- password file authentication
 - for Oracle Automatic Storage Management, [3-51](#)
 - Oracle ASM, [3-51](#)
- performance and scalability improvements for ls and find
 - enabled by compatibility attributes, [4-47](#)
- PHYS_META_REPLICATED disk group attribute, [4-5](#)
- plug-in API
 - acfsplugin, [18-7](#)
 - Oracle ACFS, [18-7](#)
 - Oracle ACFS pre-defined metric type, [18-7](#)
- plugins
 - Oracle ACFS, [11-36](#)
 - Oracle ADVM, [11-36](#)
- pre-defined metric type
 - Oracle ACFS plug-in API, [18-7](#)
- preferred read
 - failure groups, [4-37](#)
- preferred read failure groups
 - administering, [4-37](#)
- preparing security on file systems
 - Oracle ACFS, [16-7](#)
- privileges
 - ASMCMD utility, [10-8](#)
 - for one operating system group, [3-47](#)
 - Oracle ASM, [3-47](#)
 - separate operating system groups, [3-48](#)
 - SYSASM, [3-49](#)–[3-51](#)
 - SYSASM and Oracle Enterprise Manager, [7-3](#), [7-5](#)
 - SYSASM in Oracle Enterprise Manager, [7-6](#), [7-9](#)
 - SYSDBA with Oracle ASM, [3-49](#)
- PROCESSES initialization parameter
 - Oracle ASM instance, [3-13](#)
- pwdcopy command
 - ASMCMD utility, [10-16](#)
- pwdcreate command
 - ASMCMD utility, [10-16](#)
- pwd command
 - ASMCMD utility, [10-42](#)
- pwddelete command

pwddelete command (*continued*)
 ASMCMD utility, [10-17](#)
pwget command
 ASMCMD utility, [10-18](#)
pwmmove command
 ASMCMD utility, [10-19](#)
pwset command
 ASMCMD utility, [10-19](#)

Q

quorum failure group, [4-13](#)

R

READ command rule, [16-83](#)
read errors
 recovery, [4-33](#)
read-only snapshots
 enabled by compatibility attributes, [4-47](#)
read-write snapshots
 enabled by compatibility attributes, [4-47](#)
REaddir command rule, [16-83](#)
realms
 system-created security, [16-80](#)
rebal command
 ASMCMD utility, [10-61](#)
rebalance
 and CONTENT.CHECK disk group attribute, [4-23](#)
 and THIN_PROVISIONED disk group attribute, [4-23](#)
REBALANCE NOWAIT clause, [4-15](#)
REBALANCE WAIT clause, [4-15](#)
rebalancing
 disk groups, [1-12](#), [4-21](#)
rebalancing disk groups
 tuning, [4-23](#)
rebalancing process
 ASM_POWER_LIMIT initialization parameter, [3-10](#)
recommendations for storage preparation
 for Oracle ASM, [2-4](#)
recovery
 read errors, [4-33](#)
 write errors, [4-33](#)
redo logs
 creating in Oracle ASM, [17-2](#)
referencing files in the database
 Oracle ASM, [5-8](#)
regions
 intelligent data placement, [4-20](#)
registering
 Oracle ACFS file system, [16-3](#)
registry resource
 Oracle ACFS, [18-4](#)
remap command
 ASMCMD utility, [10-62](#)
REMOTE_LOGIN_PASSWORDFILE initialization
 parameter
 Oracle ASM instance, [3-13](#)
removing tag names
 Oracle ACFS, [16-13](#)
RENAME command rule, [16-83](#)
renamedg tool
 renaming disk groups, [4-57](#)
 updating resources, [4-58](#)
renaming a directory
 Oracle ASM, [5-15](#)
renaming aliases
 Oracle ASM, [5-13](#)
renaming disk groups
 renamedg and updating resources, [4-58](#)
renaming disks in a disk group, [4-18](#)
replacing disks
 altering disk groups, [4-18](#)
replacing disks in a disk group, [4-18](#)
replicated environments
 disk group compatibility considerations, [4-48](#)
replicating file systems
 calculating storage requirements, [16-13](#)
 configuring the site hosting the primary file system, [16-17](#)
 configuring the site hosting the standby file system, [16-17](#)
 managing replication background processes, [16-18](#)
 monitoring replication on the file system, [16-18](#)
 Oracle ACFS, [16-13](#)
 Oracle wallets, [16-15](#)
 pausing replication processes, [16-19](#)
 setting up tags, [16-15](#)
 unique service names for replicated file systems, [16-16](#)
 user names and service names, [16-15](#)
replication
 enabled by compatibility attributes, [4-47](#)
 Oracle ACFS, [11-30](#)
 storage requirements for Oracle ACFS file systems, [16-13](#)
 using with Oracle ACFS auditing, encryption, and security, [11-35](#)
replication status of a disk group
 enabled by compatibility attributes, [4-47](#)
resizing disks in disk groups, [4-21](#)
restricting at startup, [3-25](#)
resync
 fast mirror, [4-34](#), [7-10](#), [7-11](#)
reverting compatibility settings
 disk groups, [4-45](#)
rm command
 ASMCMD utility, [10-42](#)
rmalias command
 ASMCMD utility, [10-43](#)
RMDIR command rule, [16-83](#)
rmgrp command

- rmgrp command (*continued*)
 - ASMCMD utility, [10-75](#)
- rmtmpl command
 - ASMCMD utility, [10-66](#)
- rmusr command
 - ASMCMD utility, [10-75](#)
- rolling patches
 - Oracle ASM, [3-30](#)
- rolling upgrades
 - Oracle Automatic Storage Management, [3-29](#)
- rpusr command
 - ASMCMD utility, [10-76](#)
- running
 - ASMCMD utility, [10-6](#)
 - ASMCMD utility in a database home, [10-7](#)
 - ASMCMD utility in an Oracle grid infrastructure, [10-6](#)

S

- saving security information
 - Oracle ACFS, [16-10](#)
- scrubbing disk groups, [4-24](#)
- sector size
 - disk groups, [4-11](#)
 - enabled by compatibility attributes, [4-47](#)
 - validations for disk groups, [4-12](#)
- SECTOR_SIZE disk group attribute, [4-6](#)
- securing file systems
 - Oracle ACFS, [16-6](#)
- security
 - configuring with Oracle ASMCA, [14-5](#)
 - enabled by compatibility attributes, [4-47](#)
 - Oracle ACFS, [11-19](#)
 - Oracle ACFS and snapshots, [11-11](#)
 - system-created realms, [16-80](#)
- setattr command
 - ASMCMD utility, [10-62](#)
- setting encryption parameters
 - Oracle ACFS, [16-11](#)
- shared password file
 - for Oracle ASM instance, [3-52](#)
 - managing in a disk group, [3-52](#)
- SHARED_POOL_SIZE initialization parameter
 - Oracle ASM instance, [3-14](#)
- showclustermode command
 - ASMCMD utility, [10-20](#)
- showclusterstate command
 - ASMCMD utility, [10-20](#)
- showpatches command
 - ASMCMD utility, [10-21](#)
- showversion command
 - ASMCMD utility, [10-21](#)
- shutdown command
 - ASMCMD utility, [10-22](#)
- shutting down an Oracle ASM instance
 - about, [3-25](#)
 - with OCR or voting files in a disk group, [3-25](#)

- shutting down an Oracle ASM instance (*continued*)
 - with Oracle ACFS file system mounted, [3-26](#)
- single file creation form
 - Oracle ASM, [5-4](#)
- snapshots
 - .ACFS directory, [11-10](#), [16-125](#)
 - converting format of an existing Oracle ACFS snapshot, [11-11](#)
 - creating from existing Oracle ACFS snapshot, [11-11](#)
 - creating Oracle ACFS read-only, [16-124](#)
 - creating Oracle ACFS read-write, [16-124](#)
 - limit on the number of, [18-2](#)
 - Oracle ACFS, [11-10](#), [16-124](#), [16-126](#), [16-127](#)
 - Oracle ACFS and encryption, [11-11](#)
 - Oracle ACFS and security, [11-11](#)
 - read-write in Oracle ACFS, [11-10](#)
 - snap directory, [11-10](#)
 - snaps directory, [16-125](#)
- Solaris
 - Oracle ACFS command-line tools, [16-28](#)
- space usage
 - Oracle ACFS, [18-2](#)
- sbackup command
 - ASMCMD utility, [10-23](#)
 - backing up an Oracle ASM SPFILE, [10-23](#)
- spcopy command
 - ASMCMD utility, [10-24](#)
 - copying an Oracle ASM SPFILE, [10-24](#)
- specifying tag names for file systems
 - Oracle ACFS, [16-12](#)
- spget command
 - ASMCMD utility, [10-25](#)
 - retrieving the location of an ASM SPFILE, [10-25](#)
- spmmove command
 - ASMCMD utility, [10-25](#)
 - moving an Oracle ASM SPFILE, [10-25](#)
- spset command
 - ASMCMD utility, [10-26](#)
 - setting the location of an ASM SPFILE, [10-26](#)
- standalone server
 - Oracle Restart, [3-21](#)
- starting up an Oracle ASM instance
 - about, [3-21](#)
 - with incorrect SPFILE path, [3-24](#)
- startup
 - mounting disk groups, [3-24](#)
 - restricting disk groups, [3-25](#)
- startup command
 - ASMCMD utility, [10-27](#)
- storage considerations
 - for Oracle ASM, [2-1](#)
- storage limits
 - disk groups, [4-39](#)
 - Oracle ASM disks, [4-39](#)
 - Oracle Automatic Storage Management, [4-39](#)
- storage resources

- storage resources (*continued*)
 - disk partitions and Oracle ASM, [2-1](#)
 - for Oracle ASM, [2-1](#)
 - logical volumes and Oracle ASM, [2-1](#)
 - LUNs and Oracle ASM, [2-1](#)
 - network file systems and Oracle ASM, [2-2](#)
 - preparation for Oracle ASM, [2-2](#)
 - restrictions for Oracle ACFS, [2-2](#)
- STORAGE.TYPE disk group attribute, [4-6](#)
- storing data files and redo logs in Oracle ACFS file systems
 - enabled by compatibility attributes, [4-47](#)
- striping
 - files, [1-9](#)
 - Oracle ASM, [1-9](#)
- support for 1023 snapshots
 - enabled by compatibility attributes, [4-47](#)
- support workbench for Oracle ASM
 - Oracle Enterprise Manager, [7-29](#), [7-31](#)
- supported file types
 - Oracle ACFS, [11-1](#)
- SYMLINK command rule, [16-83](#)
- SYSASM privilege
 - accessing the Oracle ASM home page in Oracle Enterprise Manager, [7-3](#)
 - Oracle Enterprise Manager, [7-5](#), [7-6](#), [7-9](#)
- SYSDBA privilege with Oracle ASM, [3-49](#)
- system-created realms
 - security, [16-80](#)

T

- tablespaces
 - creating in Oracle ASM, [17-2](#)
- tagging
 - enabled by compatibility attributes, [4-47](#)
 - Extended Attributes requirements, [11-33](#)
 - Oracle ACFS, [11-33](#)
 - requirements for Oracle ACFS, [11-33](#)
- tagging API
 - Oracle ACFS, [18-10](#)
- tagging error values
 - Oracle ACFS, [18-11](#)
- tagging file systems
 - Oracle ACFS, [16-12](#)
- tagging name specification
 - Oracle ACFS, [18-10](#)
- template management commands
 - ASMCMD utility, [10-64](#)
- templates
 - adding to a disk group, [5-20](#)
 - attributes, [5-19](#)
 - dropping, [5-21](#)
 - for specifying redundancy and striping, [5-22](#)
 - managing Oracle ASM, [5-18](#)
 - modifying an Oracle ASM, [5-21](#)
 - Oracle ASM, [1-10](#)

- templates (*continued*)
 - user-defined for Oracle ASM, [5-22](#)
- THIN_PROVISIONED disk group attribute, [4-6](#)
- tracking the replication status
 - for disk groups, [4-5](#)
- TRUNCATE command rule, [16-83](#)
- tuning rebalance operations, [4-23](#)

U

- umount command
 - AIX, [16-40](#)
 - ASMCMD utility, [10-63](#)
 - Linux environments, [16-27](#)
 - Solaris, [16-33](#)
- umountall command
 - AIX, [16-40](#)
 - Solaris, [16-33](#)
- undropping disks in disk groups, [4-21](#)
- unlimited file system expansion
 - acfsutil size command, [16-123](#)
 - enabled by compatibility attributes, [4-47](#)
- upgrading an Oracle ASM instance
 - Oracle ASM Configuration Assistant, [9-11](#)

V

- V\$ASM_ACFS_ENCRYPTION_INFO view, [12-1](#)
- V\$ASM_ACFS_SEC_ADMIN view, [12-1](#)
- V\$ASM_ACFS_SEC_CMDRULE view, [12-2](#)
- V\$ASM_ACFS_SEC_REALM_FILTER view, [12-2](#)
- V\$ASM_ACFS_SEC_REALM_GROUP view, [12-2](#)
- V\$ASM_ACFS_SEC_REALM_USER view, [12-2](#)
- V\$ASM_ACFS_SEC_RULESET_RULE view, [12-2](#)
- V\$ASM_ACFSSNAPSHOTS view, [12-2](#)
- V\$ASM_ACFSTAG view, [12-2](#)
- V\$ASM_ACFSVOLUMES view, [12-2](#)
- V\$ASM_ALIAS view, [6-1](#)
- V\$ASM_ATTRIBUTE view
 - enabled by compatibility attributes, [4-46](#)
- V\$ASM_AUDIT_CLEAN_EVENTS view, [6-1](#), [12-2](#)
- V\$ASM_AUDIT_CLEANUP_JOBS view, [12-2](#)
- V\$ASM_AUDIT_CONFIG_PARAMS view, [6-1](#), [12-2](#)
- V\$ASM_AUDIT_LAST_ARCH_TS view, [12-2](#)
- V\$ASM_CLIENT view, [6-1](#)
- V\$ASM_DISK view, [6-2](#)
- V\$ASM_DISK_IOSTAT view, [6-2](#)
- V\$ASM_DISK_STAT view, [6-2](#)
- V\$ASM_DISKGROUP view, [4-45](#), [6-2](#)
- V\$ASM_DISKGROUP_STAT view, [6-2](#)
- V\$ASM_ESTIMATE view, [6-2](#)
- V\$ASM_FILE view, [6-2](#)
- V\$ASM_FILESYSTEM view, [12-2](#)
- V\$ASM_OPERATION view, [6-2](#)
- V\$ASM_TEMPLATE view, [6-2](#)
- V\$ASM_USER view, [6-2](#)

- V\$ASM_USERGROUP view, [6-2](#)
- V\$ASM_USERGROUP_MEMBER view, [6-2](#)
- V\$ASM_VOLUME view, [12-2](#)
- V\$ASM_VOLUME_STAT view, [12-2](#)
- variable size extents
 - enabled by compatibility attributes, [4-46](#)
- views
 - displaying Oracle ACFS information, [12-1](#)
 - displaying Oracle ASM information, [6-1](#)
- volcreate command
 - ASMCMD utility, [15-1](#)
- voldelete command
 - ASMCMD utility, [15-3](#)
- voldisable command
 - ASMCMD utility, [15-4](#)
- volenable command
 - ASMCMD utility, [15-5](#)
- volinfo command
 - ASMCMD utility, [15-5](#)
- volresize command
 - ASMCMD utility, [15-6](#)
- volset command
 - ASMCMD utility, [15-7](#)
- volstat command

- volstat command (*continued*)
 - ASMCMD utility, [15-8](#)
- volume management commands
 - ASMCMD utility, [15-1](#)
- volumes
 - enabled by compatibility attributes, [4-47](#)
- voting files in disk groups
 - enabled by compatibility attributes, [4-46](#)

W

- WAIT keyword
 - in REBALANCE clause, [4-15](#)
- wildcard characters
 - using quotes in ASMCMD commands, [10-9](#)
- WRITE command rule, [16-83](#)
- write errors
 - recovery, [4-33](#)

X

- XML DB
 - virtual folder for Oracle ASM, [5-16](#)

